VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH PRŮMYSLOVÉHO ŘEŠENÍ ISMS

DESIGN OF INDUSTRIAL SOLUTIONS ISMS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Michal Havlík
AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Michal Havlík**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh průmyslového řešení ISMS

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Závěr
Seznam použité literatury

Cíle, kterých má být dosaženo:

Práce se zabývá návrhem síťové infrastruktury ve společnosti vyrábějící součástky pro automobilový průmysl. Cílem práce je navrhnout infrastrukturu, která bude splňovat všechny podmínky stanovené pro ICS a bude vyhovovat normám pro průmyslové ISMS.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Práce se zabývá návrhem průmyslového řešení ISMS především síťové infrastruktury. V úvodu jsou uvedena teoretická východiska práce. Dále analýza současné situace v podniku a její zhodnocení. Následně samotný návrh řešení, tak aby vyhovovalo normám ISO/IEC 27 000.

Abstract

Thesis deals with industrial solutions of ISMS mainly network infrastructure. First introduction into theoretical background of the thesis. Further analysis of the current situation in the company and its evaluation. Consequently, the design of solution done to meet the standards of ISO / IEC 27000.

Klíčová slova

ISMS, průmyslové řešení, ISO/IEC 27000, bezpečnost, systém řízení bezpečnosti informací

Keywords

ISMS, industrial solution, ISO/IEC 27000, security, information security management systém

Bibliografická citace

HAVLÍK, M. *Návrh průmyslového řešení ISMS.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 69 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 23. května 2017 …….....

Michal Havlík

PODĚKOVÁNÍ

Děkuji panu Ing. Petru Sedlákovi za vedení této práce a své rodině a přátelům za podporu při studiích.

Obsah

ÚVOD

Jak jde čas, tak jde i pokrok kupředu. V oblasti IT je tento pokrok daleko znatelnější než v jiných oblastech. Výpočetní výkon stále roste, všude se setkáváme s digitalizací dat a informací. S ním roste i možnost jejich zneužití.

Tento problém se týká i oblasti firem, podniků a různých organizací. Společnosti jsou ze zákona povinny chránit údaje o zaměstnancích, dodavatelích a odběratelích. Každá společnost si zároveň musí chránit i své know-how. Proto je potřeba zavádět systém řízení informační bezpečnosti (zkráceně ISMS). Doporučení pro zabezpečení jsou shrnuta v normách řady ISO/IEC 27000, ve kterých jsou shrnuty postupy pro zavedení ISMS a jak chránit důležitá data a důležité informace.

1 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Práce se zabývá návrhem síťové infrastruktury ve společnosti vyrábějící součástky pro automobilový průmysl. Cílem práce je navrhnout infrastrukturu, která bude splňovat všechny podmínky stanovené pro ICS a bude vyhovovat normám pro průmyslové ISMS.

2 TEORETICKÁ VÝCHODISKA

Nejdříve si vysvětlíme základní pojmy spojené s informační bezpečností a její normy. Po vysvětlení základů si přiblížíme informační bezpečnost v průmyslovém prostředí. Na konci diplomové práce lze najít seznam použitých zkratek a jejich stručné vysvětlení.

2.1 Základní pojmy a názvosloví

Níže jsou vypsány jednotlivé pojmy a jejich vysvětlení:

- **Informace** - širší pojem, který popisuje reálné prostředí, jeho stav i procesy v něm probíhající ve formě údajů.
- **Data** - jsou plněním informace, kterou vytváří.
- **Přenos dat** - je přenos digitálních zpráv nebo digitalizovaného analogového signálu, a to pomocí fyzického dvoubodového či vícebodového přenosového prostředí (metalický kabel, optický kabel, bezdrátový přenos).
- **Síťová infrastruktura** - tento pojem zahrnuje veškeré síťové prvky a zařízení použité při realizaci komunikační sítě.
- **Počítačová síť** - je součástí síťové infrastruktury a slouží k realizaci komunikačního prostředí mezi uživateli.
- **ISMS** – Information Security Management System, systém řízení informační bezpečnosti.
- **Bezpečnost informací** - zachování důvěrnosti, dostupnosti a integrity informací.
- **Důvěrnost** - zajištění přístupnosti k informaci pouze oprávněnému uživateli.
- **Dostupnost** - zajištění přístupnosti k informaci oprávněnému uživateli v požadovaný okamžik.
- **Integrita** – zajištění správnosti a úplnosti informace.
- **Aktivum** – veškerý nehmotný a hmotný majetek společnosti.
- **Hrozba** – událost, která ohrožuje bezpečnost.
- **Zranitelnost** – slabé místo aktiva.
- **Opatření** – aktivita, která umožňuje snížení hrozby.
- **Riziko** – kombinace zranitelnosti a hrozby s dopadem na aktivum.
- **Dopad** – vznik škody v důsledku působení hrozby.

- **Řízení rizik** - koordinace, která je nutná k řízení a kontrole organizace s ohledem na rizika.
- **Analýza rizik** - systematické používání informací pro odhad míry rizika a také k určení jeho zdrojů.
- **Akceptace rizika** – rozhodnutí o přijetí rizika.
- **Prohlášení o aplikovatelnosti** – dokument, který popisuje opatření ISMS v organizaci.

2.2 Normy pro ISMS

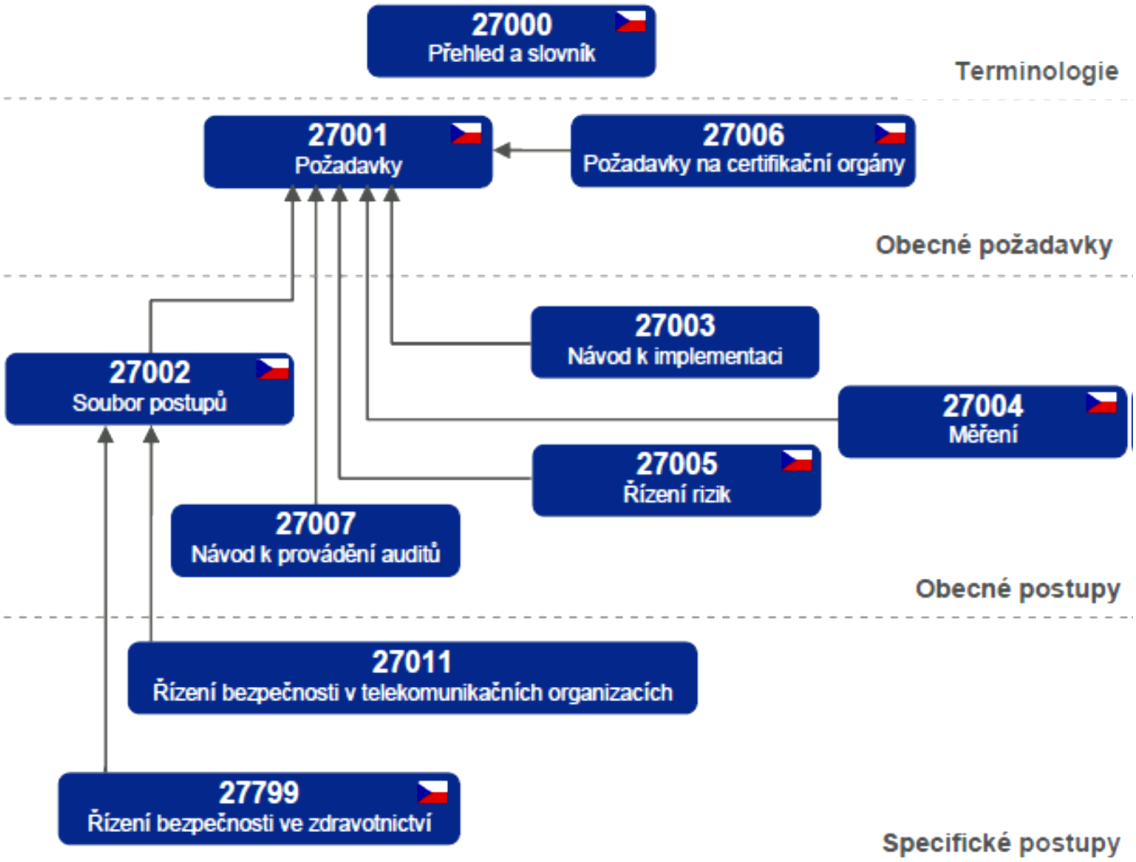
2.2.1 Normy ISO/IEC 27000

Tato řada norem popisuje řízení bezpečnosti informací v organizacích:

- **ISO/IEC 27000** – přehled a slovník
- **ISO/IEC 27001** – požadavky
- **ISO/IEC 27002** – soubor postupů pro opatření bezpečnosti informací
- **ISO/IEC 27003** – směrnice pro implementaci systému řízení bezpečnosti informací
- **ISO/IEC 27004** – měření
- **ISO/IEC 27005** – řízení rizik bezpečnosti informací
- **ISO/IEC 27006** – požadavky na orgány, které provádějí audit a certifikaci systému řízení bezpečnosti informací
- **ISO/IEC 27007** – směrnice pro audit ISMS
- **ISO/IEC 27008** – směrnice pro audit opatření ISMS
- **ISO/IEC 27010** – směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi
- **ISO/IEC 27011** – směrnice pro řízení bezpečnosti informací pro telekomunikační organizace
- **ISO/IEC 27013** – návod pro integrovanou implementaci ISO/IEC 27001
- **ISO/IEC 27014** – správa bezpečnosti informací
- **ISO/IEC 27015** – směrnice pro řízení bezpečnosti informací pro finanční služby

- **ISO/IEC 27016** – řízení bezpečnosti informací pro organizační ekonomiku

Na následujícím schématu lze vidět provázanost jednotlivých směrnic.



Obrázek 1: Struktura norem řady 27000, Zdroj: [11]

2.3 Definice, klasifikace a hodnocení aktiva

Aktivum je cizí slovo pro majetek, kde se jedná o veškerý hmotný i nehmotný majetek. Pro ohodnocení aktiv je třeba si nejprve aktiva identifikovat. Vytvořit skupiny aktiv, která k sobě patří (programová aktiva, bezpečnostní aktiva, obchodní aktiva apod.). Dále identifikovat vlastníka (pověřenou osobu, která je plně zodpovědná za dané aktivum) každého aktiva, se kterým se následně určuje konkrétní hodnota aktiva [1].

K hodnocení aktiv, lze přistoupit mnoha způsoby. Můžeme využít softwarový nástroj, který je k tomu přímo určený nebo si aktiva sepsat do tabulky, např. v Excelu. Dále si musíme stanovit hodnotící kritéria a stupnici ke každému aktivu. Vyjádření stupnice může být buď v peněžní, nebo kvalitativní hodnotě aktiva. Volba je na vedení společnosti.

Peněžní stupnice vyjadřuje v místní měně hodnotu určitého aktiva. Kvalitativní vyjádření určuje hodnotu v termínech, např. stupnice od velmi nízké, až po kritické [1].

Je potřeba si každou hodnotu stupnice vhodně „obarvit“. Barevné označení nám pomůže při orientaci v rozsáhlých seznamech aktiv. Společnost si zvolí výběr a rozsah termínů, výběr také závisí na bezpečnostních potřebách organizace, její velikosti a dalších aspektech. K hodnocení aktiv lze využít systém řízení kvality (ISO 9001), pokud jej má společnost zavedený. Hodnotí se náklady, které by mohli vzniknout při porušení dostupnosti, důvěrnosti a integrity aktiva. Tato tři kritéria nám poskytují podklady pro ohodnocení aktiv [1].

Hodnocení aktiv musí probíhat ve spolupráci s majitelem aktiva. Jeho subjektivní pohled je potřeba prodiskutovat i s uživatelem aktiva, který může přinést další užitečné poznatky. Křížová kontrola je velmi důležitá k upřesnění hodnoty aktiva. Tato kontrola by měla být provedena u všech aktiv, která mají pro organizaci vysokou hodnotu [1].

2.4 Bezpečnostní hrozby

Hrozba má potenciální schopnost způsobit nežádoucí incident. Tento incident může mít za následek poničení systému nebo organizace, popř. jejich aktiv [1].

2.4.1 Základní rozdělení hrozeb

Dle původu:

- **Přírodní** – požár, povodně, zemětřesení.
- **Způsobené lidským faktorem** – odposlech, chyba uživatele.

Dle úmyslu:

- **Náhodné** – zapomenuté dokumenty s důvěrnými daty, vymazání souboru.
- **Úmyslné** – úmyslné poškození, krádež.

Z hlediska bezpečnosti je nutné, identifikovat náhodné i úmyslné hrozby a odhadnout jejich úroveň a pravděpodobnost [1].

Hrozby můžeme dělit i podle toho, na jaké aktivum působí [1]:

- **Operační systém**
- **Aplikace**
- **Databáze**
- **Síť**
- **Klient**

2.4.2 Posouzení hrozeb

Hrozby posuzujeme vždy na základě následujících otázek [1]:

- Ztráta důvěrnosti – může vést ke ztrátě důvěry vůči zákazníkům, právní odpovědnosti, finanční ztrátě apod.
- Ztráta integrity – může vést k přijetí nesprávných rozhodnutí.
- Ztráta dostupnosti – může vést k neschopnosti vykonávat kritické činnosti.
- Ztráta individuální odpovědnosti – může vést k podvodu, špionáži, krádeži.
- Ztráta autentičnosti – může vést k použití neplatných dat, která vedou k neplatným výsledkům.
- Ztráta spolehlivosti – může vést k nespolehlivým dodavatelům, demotivaci zaměstnanců.

Nesmíme zapomenout na následné efekty hrozby. Vezměme si příklad výpadku elektrické energie. Za následek nemusí být pouze nedostupnost dat, ale dlouhodobý výpadek může vést k ohrožení činnosti organizace, nebo ohrožení lidského života (nemocnice, hasiči, policie) [1].

Mezi nejčastější hrozby můžeme řadit [1]:

- Selhání dodávky energie
- Škodlivý software
- Selhání hardwaru
- Selhání komunikačních služeb

2.5 Analýza rizik

Analýzu rizik provádíme za účelem zjištění zranitelných míst ve společnosti. Tato analýza stanovuje rizika, která jsou příslušná každému zranitelnému místu a hrozbě, a také zachycuje hrozby, které působí na informační systém [1].

Pokud se řekne riziko, rozumí se tím nebezpečí vzniku škody, poškození, ztráty, zničení aktiva nebo dat. Tuto skutečnost lze chápat jako možnost odlišného a hlavně nežádoucího vývoje od předpokládaného [2].

Rizika rozlišujeme na [1]:

- **Bezvýznamné riziko** – není vyžadováno žádné zvláštní opatření. Riziko lze přijmout.
- **Akceptovatelné riziko** – přijatelné se souhlasem vedení. Nutno zvážit náklady na případné řešení nebo zlepšení.
- **Mírné riziko** – urgentnost opatření není tak závažná jako u nežádoucích rizik, ovšem je nutno zpravidla bezpečnostní opatření zrealizovat dle zpracovaného plánu vedení firmy. Potřeba nápravné činnosti.
- **Nežádoucí riziko** – tento typ rizika vyžaduje urychlené provedení odpovídajících bezpečnostních opatření, které by riziko snížilo na přijatelnější úroveň. Vyžaduje bezprostřední bezpečnostní opatření.
- **Nepřijatelné riziko** – jak je již z názvu patrné, jedná se o nepřípustné, kritické riziko. Nutnost okamžitého zastavení činnosti, odstavení z provozu do doby, než se provedou nezbytná opatření. Práce se nesmí zahájit, nebo pokračovat, dokud se riziko nesníží.

V následující kapitole si popíšeme jednotlivé kroky analýzy rizik.

2.5.1 Stanovení hranic revize

Zhotovíme ještě před identifikací a hodnocením aktiv. Pokud toto provedeme pečlivě, umožní nám to vyvarovat se zbytečných činností a ušetří nám čas. Budeme tedy definovat, kterých prvků se analýza rizik bude týkat (např. HW, SW) [1].

2.5.2 Identifikace a ohodnocení aktiv

Tato problematika již byla popsána v kapitole **2.3**.

2.5.3 Hodnocení hrozeb

Tato problematika již byla popsána v kapitole **2.4**.

2.5.4 Odhad zranitelnosti

Odhalení slabých míst ve fyzickém prostředí, organizaci, postupech, personálu, managementu, administraci hardware, software nebo v komunikačním zařízení. Tato místa pak mohou být zneužita a způsobit tak škodu na aktivech [1].

2.5.5 Identifikace plánovaných a existujících ochranných opatření

Součást analýzy rizik. Výsledkem tohoto kroku je seznam existujících a plánovaných bezpečnostních opatření [1].

2.5.6 Výběr ochranných opatření

Slouží k minimalizaci případných rizik. Usnadněné popisy různých typů ochranných opatření, jsou zavedeny v rámci normy kategorie ochranných opatření. Mezi nejdůležitější patří tzv. všeobecně aplikovatelná ochranná opatření [1].

Základní kategorie ochranných opatření [1]:

- Řízení a politiky bezpečnosti IT
- Kontrola bezpečnostní shody
- Řešení incidentů
- Personální opatření
- Provozní problémy
- Plánování kontinuity činnosti organizace
- Fyzická bezpečnost

2.5.7 Odhad rizik

Slouží k identifikaci a odhadu rizik, která ohrožují aktiva. Říká nám, co a proč nám hrozí [1].

2.5.8 Přijetí rizik

Po provedení předchozích kroků nám zůstávají na seznamu zbytková rizika. Neexistuje nic jako úplně bezpečný systém. To je pouze teoretické východisko, ke kterému se snažíme v reálném provozu přiblížit. Tato zbytková rizika se dělí na rizika akceptovaná a neakceptovaná. Pokud riziko neakceptujeme, musí znovu proběhnout výběr ochranných opatření a odhad rizika [1].

2.5.9 Politika bezpečnosti systému IT

Obsahuje podrobnosti požadovaných ochranných opatření a také jejich popis, proč jsou nezbytná [1].

2.5.10 Plán bezpečnosti IT

Dokument, který popisuje veškeré akce nezbytné k tomu, aby mohla být ochranná opatření implementována [1].

2.6 Management bezpečnosti pasivní vrstvy

Management pasivní vrstvy využívá kombinaci softwaru, elektroniky a produktů strukturované kabeláže. Umožňuje uživatelům sledování a správu jejich investic od fáze plánování, přes návrhy, instalaci, až po případný upgrade infrastruktury. Typickým příkladem Managementu bezpečnosti pasivní vrstvy je NISS (Network Infrastructure Security Solution) a definuje tři stupně zabezpečení [1].

2.6.1 Stupeň 0 – identifikátory

Stupeň 0 neposkytuje fyzickou ochranu komunikace. Usnadňuje orientaci a přehled v zapojení sítě, díky barevnému rozlišení jednotlivých prvků. Jestliže chceme tento systém aplikovat na stávající síť, pak použijeme barevné kroužky nebo popisové štítky. Pokud bychom budovali novou pasivní vrstvu, lze využít barevných propojovacích kabelů. [1].

Základními identifikačními prvky jsou [1]:

- Barevné propojovací kabely
- Barevné značkovací kroužky, popisovací štítky

Obrázek 2: Barevné značkovací kroužky, propojovací kabel, Zdroj: [1]

2.6.2 Stupeň 1 – blokátory

Tento stupeň už zajišťuje základní fyzickou ochranu. Blokuje porty (proti připojení, nebo proti odpojení) a blokuje přístup (do kabelových tras a datových boxů). Funguje tak, že se blokátor zasune do blokovaného portu, či nasadí na blokovaný konektor a sundat jej lze pouze za použití speciálního klíče [1].

Blokátory dělíme na [1]:

- Blokování portu (datového metalického, optického nebo USB portu)
- Uzamčení portu proti neoprávněnému odpojení
- Blokování datového boxu proti neoprávněnému přístupu a připojení nežádoucího zařízení
- Blokování kabelových tras proti neoprávněnému přístupu ke kabelovým svazkům

Obrázek 3: Blokátor optického LC konektoru a datového portu RJ-45, Zdroj: [1]

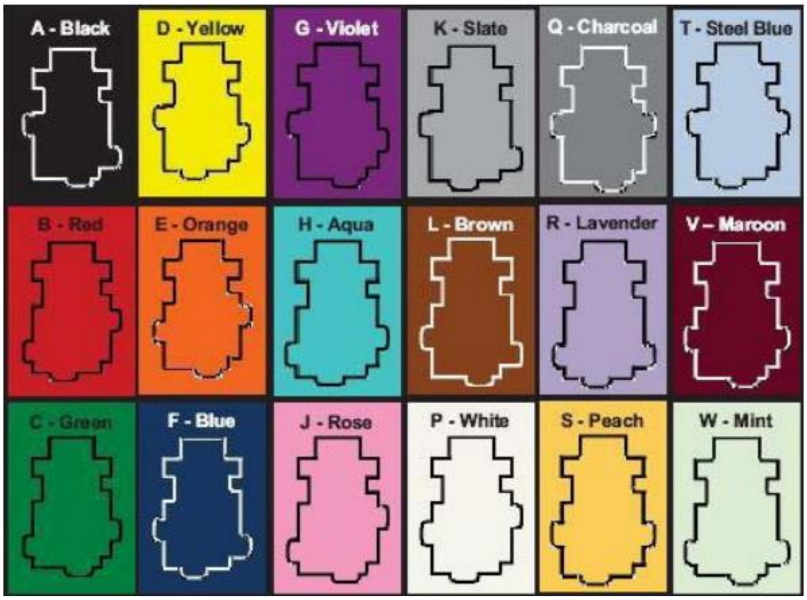
2.6.3 Stupeň 2 – klíčování konektorů

V tomto stupni je zamezeno připojení metalických propojovacích kabelů a optických duplexních propojovacích kabelů do nepovolených portů. Jedná se o technické řešení využívající klíčování konektorů. Klíčování je řešeno různým tvarováním portů a příslušných konektorů v trojrozměrném provedení[1].

Princip bezpečnostního opatření je postaven na následujících bodech [1]:

- Neklíčovaný plug nelze zasunout do žádného klíčovaného jacku
- Klíčovaný plug nelze zasunout do neklíčovaného jacku, ani do jacku s jiným typem klíče

Stejný princip platí také pro optické konektory.



Obrázek 4: Různé tvary klíčování LC portu, Zdroj: [1]

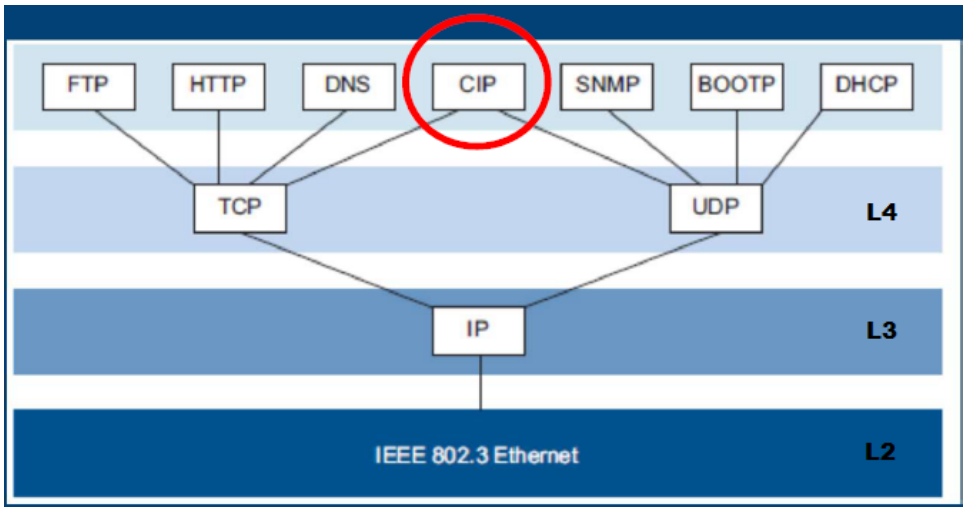
2.7 Průmyslová bezpečnost

Bezpečnost v průmyslu je zkráceným názvem pojmu bezpečnost průmyslového prostředí ICT. Bezpečnost ICT v průmyslu je klíčovým prvkem a je dosahována maximálními možnostmi aplikovaných doporučených bezpečnostních doporučení. Základním parametrem průmyslových aplikací je práce v reálném čase, proto jsou požadavky na průmyslovou síťovou infrastrukturu tak specifické a nekompromisní. Tímto splňuje průmyslová infrastruktura také požadavky na síť s maximální dostupností [1].

2.7.1 Industrial Ethernet

Protokol EtherNet/IP byl založen na bázi Ethernetu. EtherNet/IP byl celosvětově standardizován jako průmyslový komunikační protokol. Protokol využívá standardizovaných transportních protokolů TCP/IP a UDP/IP [1].

Pro potřeby průmyslu byl vytvořen protokol CIP. CIP (Common Industrial Protocol) pracuje na bázi EtherNet/IP a rozšiřuje ethernetovské použití pro oblast aplikací pro průmyslovou automatizaci [1].



Obrázek 5: Ethernet CIP v referenčním ISO/OSI modelu, Zdroj: [7]

2.8 Parametry průmyslové síťové infrastruktury

Typické parametry jsou zakotveny a zabudovány v samotné standardizaci Industrial Ethernet [1].

Tato zařízení jsou určená pro nasazení ve specifických podmínkách [1]:

- Teplotní odolnost
- Odolnost vůči vodě a vlhku
- Odolnost vůči agresivnímu prostředí
- Odolnost vůči mechanickým vlivům
- Odolnost vůči elektromagnetickému rušení

Veškeré tyto požadavky se následně projeví na konstrukci jednotlivých komponentů v pasivní i aktivní vrstvě. [1].

Prvky pasivní vrstvy [1]:

- **Kabely** – zodolněné, speciální či s pancéřovaným plášťováním.
- **Konektory** – standardní v odolném provedení (krytí) nebo speciální (např. M12).
- **Datové rozvaděče** – 19“ ve specifickém provedení či s lištami DIN.

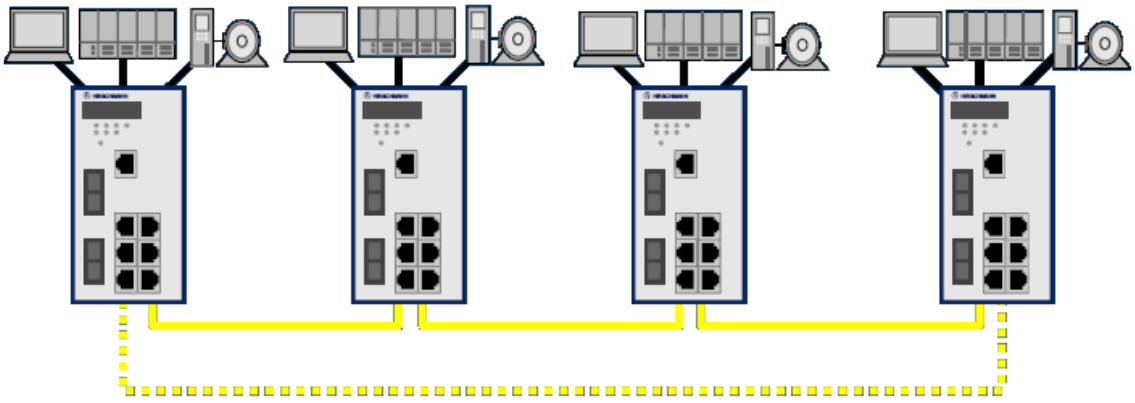
Aktivní prvky [1]:

- Bezventilátorové provedení
- Provedené pro montáž na DIN lišty
- „Coating“ elektroniky (máčení ve speciálních odolných lacích)
- Speciální odolné vodotěsné plášťování

2.8.1 Topologie

Topologie v průmyslovém prostředí byla dříve na sériové komunikaci (sběrnicová topologie), poté přichází Ethernet/IP pro průmysl (topologie hvězda) a na závěr při požadavku na topologickou redundanci vznikla kruhová topologie s různými úrovněmi zabezpečení [1].

V dnešní době je standardní průmyslová topologie ve většině případů kruhová (ring). Vzniká z liniové topologie, a to tak, že se propojí počáteční a koncové zařízení, viz následující obrázek [1].



Obrázek 6: Vznik kruhové topologie pomocí redundantní trasy, Zdroj: [3]

Rozšiřování kruhové topologie může být řešeno několika způsoby [1]:

- Napojením dalších kruhů (Sub-ring) na zařízení v hlavním kruhu
- Napojením kruhů pomocí linek v redundantním provedení – Couplink
- V některých případech se používá typická topologie hvězdy při napojení na koncové přepínače

2.8.2 Redundance

Redundance je volně přeložena jako nadbytečnost, ale v průmyslovém prostředí má své opodstatnění, protože zajišťuje bezpečnost a dostupnost sítě [1].

Výběrová kritéria pro volbu redundance [1]:

- Použití napojení pomocí jednoho zařízení je úsporné, ale při výpadku tohoto zařízení není napojení mezi sítěmi.
- Použití napojení pomocí dvou zařízení je praktičtější, jelikož při výpadku kteréhokoli zařízení stále existuje napojení.
- Použití napojení pomocí dvou zařízení s kontrolní linkou nemá žádný vliv na provoz v žádném kruhu. Řeší pouze komunikaci mezi redundantními zařízeními.

Redundance topologická

Kruh je základní topologie u linkových tras. Ten vzniká, uzavřením linkové topologie redundantní trasou, která byla blíže vysvětlena v kapitole **2.8.1**.

Základní parametry pro kruhovou topologii [1]:

- Síťová vzdálenost 3000 km
- Vzdálenost mezi dvěma zařízeními do 120 km
- Doba reakce dle základního nastavení menší než 10 ms nebo menší než 200 ms
- Síť může obsahovat cca 50 zařízení typu switch
- Pracuje na sítích 10 Mbps až 10 Gbps

Redundance zařízení

Základem je redundance zařízení při napojení dvou kruhů pomocí kontrolní linky. Extrémní redundantní zapojení je paralelní, neboli duplikovaná síť. Tato redundance je podporována na všech úrovních [1].

Redundance napájení

Většinou řešena různými způsoby napájení průmyslových ICT zařízení [1]:

- Zdvojené standardní napájení 230 V/50 Hz v rozsahu 90 až 265 V AC – typicky zdroje
- Napájení 24 nebo 48 DC v rozsahu 18 až 60 V
- Kombinace napájení AC a DC s automatikou, neboli přepínaní

2.9 Mission Critical Network

Pojmem Mission Critical je označený požadavek na plně funkční systémy, které jsou životně důležité pro fungování organizace. Mission Critical Network je označení pro komunikační sítě [2].

Mission Critical Network má tři základní pravidla [1]:

- **Jednoduchost**
- **Separátní rutinní provoz**
- **Spolehlivost**

Jednoduchost

Snížení komplexního použití v návrhu síťové infrastruktury. Zrychlení odstraňování závad a údržba sítě. Snížení rizika za pomoci snížení komplexnosti infrastruktury a nákladů na školení uživatelů. Předcházení lidským chybám.

Separátní rutinní provoz

Logické oddělení sítí s odlišným použitím. Správa šířky přenosového pásma. Izolování vadných či nespolehlivých aplikací.

Spolehlivost

Činnost síťové infrastruktury ve ztížených podmínkách. Minimální výpadky sítě. Životnost síťové infrastruktury minimálně 15 let. Nadčasovost. Dosažení maximální dostupnosti.

Požadavky na odolnost systému vůči vlivům prostředí [2]:

- **Rozsah pracovních teplot** – komerční prvky 5 – 40 °C / MCN 0 – 60 °C nebo -40 – 70 °C, někdy i více
- **Odolnost proti chemickým vlivům prostředí –** vlhkost, voda, olej, benzín, odmašťovadla a působení dalších chemikálií. To vše jsou vlivy, kvůli kterým jsou kladeny vysoké nároky na odolnost prvků. Klade se důraz na vysokou odolnost plášťů kabelů a konektorů. U aktivních prvků je ochrana prováděna speciálním lakem (coating).
- **Odolnost vůči povětrnostním podmínkám** – vlhkost, voda, prašnost, UV záření.
- **Odolnost vůči ostatním vlivům prostředí** – vibrace a rázy, ultrazvuk, radiace a rentgenové záření.

2.10 Propojení sítí se zabezpečeným oddělením

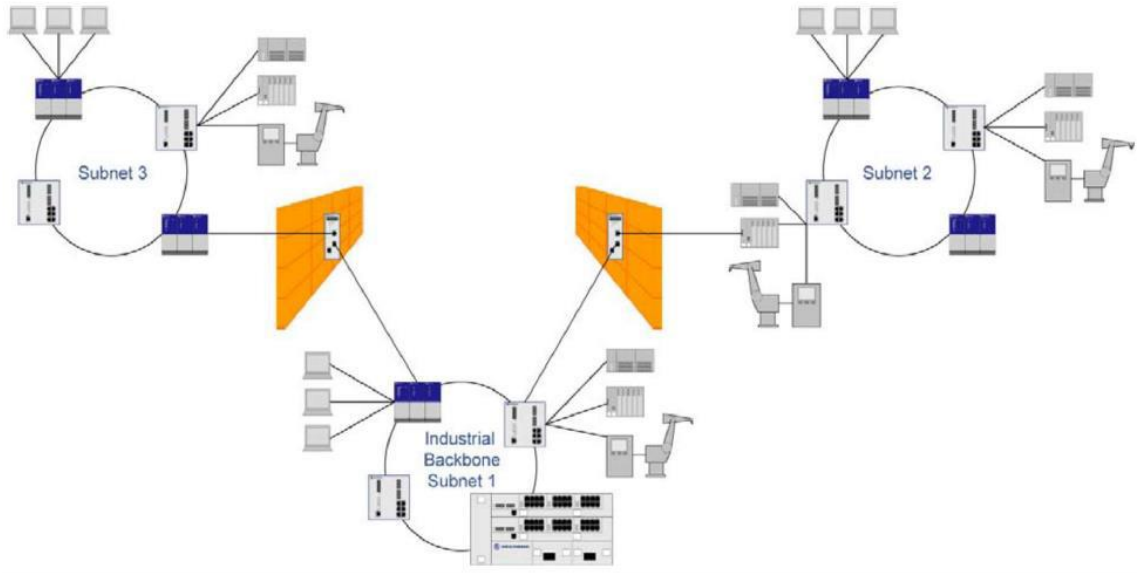
Integrovanou komunikační infrastrukturu podniku navrhujeme jako fyzicky oddělené sítě se vzájemným zabezpečeným propojením. Pro připojení do vnějších veřejných sítí, můžeme u většiny případů použít pro oddělení sítí router nebo firewall. Pro oddělení sub-sítí v rámci hierarchické infrastruktury se používají aplikační firewally [4].

V rámci typické struktury integrované sítě podniku potřebujeme mít často lokálně zabezpečená připojení, např. pro údržbu, diagnostiky apod. V mnoha případech je dobré mít takové zabezpečené připojení i se vzdáleným přístupem, což urychlí diagnostiku a není potřeba čekat na příchod servisního technika. Kolikrát se může stát, že servisní technik na dálku zjistí, že žádná porucha nenastala a stav zařízení byl vyvolán chybou obsluhy. Takovýmto způsobem uvede zařízení do správného stavu nebo informuje obsluhu o případných úkonech [4].

Integrovanou podnikovou komunikační infrastrukturu je potřebné oddělit nejen z pohledu aplikačního, ale i z hlediska systémového členění vnějších a vnitřních napojení. Jednotlivé sub-sítě se většinou oddělují pomocí aplikačních firewallů. To platí především v případech oddělení řízení kritických aplikací od administrativní sítě nebo kritického výrobního procesu [4].

2.11 Zónové zabezpečení

Pomocí zónového zabezpečení se rozdělí síť na pracovní skupiny, které mají něco společného a ty se navzájem ještě oddělí. Každá skupina má svou vlastní správu, která je platná jenom pro tu danou skupinu. Zónové zabezpečení je důležité v případech, kdy máme zařízení od různých výrobců a každé má jiné nastavení [3].



Obrázek 7: Příklad zónového zabezpečení, Zdroj: [7]

3 ANALÝZA SOUČASNÉHO STAVU

Tato kapitola popisuje současný stav v podniku. Zmapuje síťovou infrastrukturu a celkovou bezpečnost. Jedná se o stejnou společnost, u které vznikala moje bakalářská práce. Společnost si nepřeje být jmenována.

3.1 Popis společnosti

Společnost ABC má sídlo ve Švýcarsku a její česká větev se zaměřuje na výrobu rozbušek do automobilových airbagů. Kromě toho se zde vyrábějí další bezpečnostní prvky do automobilů. Největšími odběrateli jsou koncerny General Motors a Volkswagen.

Jelikož manipulují s výbušninami, jsou v této společnosti zavedeny velmi přísné bezpečnostní předpisy a je kladen důraz na přesnost. Proto si nemůže dovolit dostávat nepřesné nebo nekompletní informace, nemluvě o jejich ztrátě. Každý den probíhá kontrola reportů, které vytvářejí jednotlivé pneumatické výrobní linky a pokud jsou nepřesné, znamená to pro společnost vysoké náklady na investigaci a nápravu.

V České republice má asi 70 zaměstnanců a v současné době realizuje modernizaci komunikační infrastruktury. To zahrnuje i modernizaci síťové infrastruktury ve výrobním prostředí. O výrobu se stará ICT tým, který má zároveň na starost i komerční infrastrukturu.

Společnost je rozdělená do dvou hlavních budov, které jsou od sebe vzdálené 20m, dále se v areálu nacházejí tzv. „bunkry“ (sklady a přípravna výbušnin).

3.2 Popis infrastruktury

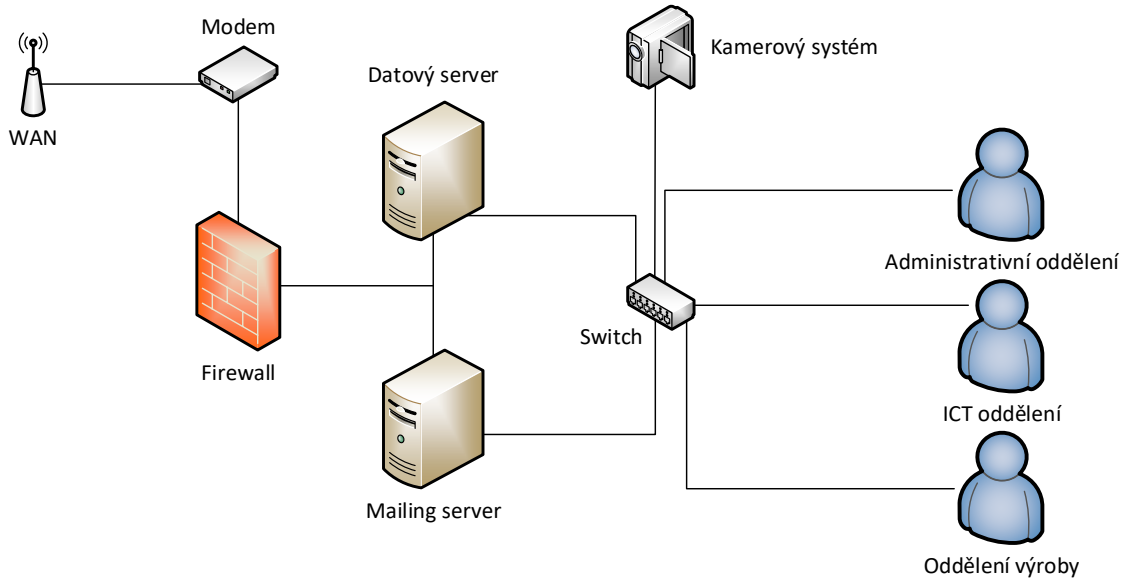
Celá infrastruktura vznikala během projektu, kdy se budovala česká větev společnosti. Na průmyslové řešení se nedbalo, a proto je celá síť vybudovaná z komerčních prvků.

Pro kabeláž byly využity metalické UTP kabely a plastové koncovky. Pro vedení kabeláže se nepoužilo nic. Kabely jsou svázané a položené buď podél zdi, nebo visí na protipožární konstrukci na stropě. Toto řešení neposkytuje jakoukoli ochranu a tím pádem nesplňuje požadavky na průmyslovou bezpečnost. Každý má k takové kabeláži přístup a může ji lehce poškodit.

Aktivní prvky jsou taktéž komerční. Většinou výrobky od společnosti Juniper nebo Cisco. U výrobních linek se s chemikáliemi nepracuje, ale v přípravně a kontrolní laboratoři ano. Prvky nejsou vůči těmto vlivům chráněné. Pro uložení prvků je použit datový rozvaděč s ventilátorem. Toto řešení taktéž nesplňuje požadavky na průmyslovou bezpečnost.

Komunikace s vnějším světem zajišťuje připojení od poskytovatele T-mobile. Za firewallem jsou servery (datový a poštovní), ale průmyslová a administrativní část od sebe nejsou oddělené, což je velká slabina a potencionální útočník by byl schopen ukrást nejen administrativní data, ale i ta průmyslová. Tím by mohl společnost připravit o miliony korun.

Výrobní linky ovládají PLC, které ovládají pracovníci skrze pracovní stanice, které nejsou příliš zabezpečené. Spoléhá se na „omezený přístup“, který zajišťují přístupové čipy a politika přístupů. Pokud se už dostane člověk za dveře, má volný přístup ke stanicím. Opět nejsou splněny podmínky pro průmyslovou bezpečnost.



Obrázek 8: Schéma síťové infrastruktury ve společnosti, Zdroj: [Vlastní]

3.3 Zhodnocení současného stavu

Podle mého názoru má společnost v oblasti průmyslové bezpečnosti obrovské nedostatky.

Kabeláž je nechráněná proti vnějším vlivům. Jsou použity komerční materiály, které nejsou stavěné pro agresivní prostředí průmyslu. Ten samý nedostatek vidím i u prvků aktivní vrstvy.

Dále je potřeba zajistit kontrolu přístupů, kvůli úniku citlivých dat a zařadit účinnější firewall, který bude oddělovat administrativní část od té průmyslové a zároveň bude provádět hloubkovou kontrolu paketů, aby tak zabránil napadení malwarem.

4 VLASTNÍ NÁVRHY

V této části práce se budeme zabývat samotným návrhem nové síťové infrastruktury a řízení informační bezpečnosti, tak aby vše vyhovovalo normám ISO 27000. Návrh bude zahrnovat pasivní vrstvu, aktivní vrstvu, řídící software a nejkritičtější části ISMS.

4.1 Analýza rizik

V této části kapitoly provedeme identifikaci a ohodnocení rizik a zranitelností. Sestavíme matici hrozeb a stanovíme míru rizik.

4.1.1 Identifikace a ohodnocení aktiv

Nejdříve je potřeba udělat si seznam všech aktiv, která je potřeba chránit. Zároveň je potřeba si stanovit jaký dopad bude mít na společnost jejich poškození nebo případné vyřazení z provozu. V tomto případě použijeme slovní metodu hodnocení aktiv.

Pro tento případ volíme stupnici hodnocení aktiv následovně:

Hodnota aktiva	Hodnota slovy	Dopad na společnost
1	Nevýznamné	Nemá dopad na chod společnosti, nízké náklady
2	Méně významné	Lehký dopad na společnost, aktivum s určitou hodnotou
3	Významné	Znatelný dopad na společnost, hrozí finanční ztráty, možné omezení chodu společnosti
4	Cenné	Vysoká hodnota dopadu pro společnost, vážné problémy pro chod společnosti
5	Velmi cenné	Dopad může být fatální pro společnost, klíčová aktiva

Tabulka 1: Slovní hodnocení aktiv, Zdroj: [Vlastní]

Dále si musíme sestavit seznam všech aktiv, která chceme chránit. Rozdělíme si je do třech kategorií: Data, Hardware a Software. Nebudeme uvádět všechna aktiva společnosti, pouze ty nejdůležitější.

Aktivum	Zdroj	Hodnota
Data	IS data	5
	Data	5
	Zálohy	4
	DB data	5
	Reporty	4
Hardware	Server	4
	PC	2
	PLC	4
	Linky	5
	Kamery	3
	NAS	4
	Přístupový systém	4
	Síťová infrastruktura	5
SW	OS	1
	Office	2

Tabulka 2: Seznam a hodnocení aktiv, Zdroj: [Vlastní]

Hodnotíme jejich dopad na integritu, dostupnost a důvěrnost. Pro výpočet hodnoty aktiva jsme použili následující vzoreček:

$$Hodnota\ aktiva = \frac{Dostupnost + Důvěrnost + Integrita}{3}$$

Obrázek 9: Vzoreček pro výpočet hodnoty aktiva, Zdroj: [1]

4.1.2 Identifikace hrozeb a zranitelností

V následující tabulce je slovní hodnocení hrozeb. To potřebujeme k sestavení matice zranitelností. V tabulce je zapsána pravděpodobnost, s jakou může hrozba nastat, její dopad na společnost a význam rizika.

Pravděpodobnost	Dopad na společnost	Význam
1	Žádný dopad na společnost	Bezvýznamné riziko
2	Zanedbatelný dopad	Akceptovatelné riziko
3	Potíže či finanční ztráty	Mírné riziko
4	Vážné potíže či velké finanční ztráty	Nežádoucí riziko
5	Existenční potíže	Nepřijatelné riziko

Tabulka 3: Hodnocení hrozeb, Zdroj: [Vlastní]

Po poradě s IT týmem společnosti, konzultaci s vedoucím práce a literaturou jsme vybrali nejdůležitější hrozby, které by mohli výrazně ovlivnit chod společnosti. Většina standartních hrozeb byla převzata z normy ČSN ISO/IEC 27005. Hrozby jsou rozděleny do různých kategorií, jsou slovně popsány a je uvedena pravděpodobnost jejich výskytu.

Hrozba			Pravděpodobnost
Fyzické poškození	1	Požár	2
	2	Voda	1
	3	Prach	2
	4	Chemikálie	3
	5	Destrukce zařízení	2
	6	Exploze	2
Dostupnost služeb	7	Výpadek elektrické energie	3
	8	Výpadek internetu	4
	9	Výpadek IS	3
	10	Výpadek serveru	2
	11	Výpadek interní sítě	3
Důvěrnost služeb	12	Neoprávněný přístup do sítě	3
	13	Neoprávněný přístup do IS	3
	14	Neoprávněný přístup na server	3
	15	Škodlivý software	4
	16	Zneužití nebo krádež disků	2
	17	Krádež technického vybavení	3
	18	Získání dat z vyřazených médií	2
Technické selhání	19	Selhání serverů	3
	20	Selhání pracovních stanic	3
	21	Selhání PLC	4
	22	Selhání výrobních linek	4
	23	Selhání zálohovacího systému	2
	24	Selhání prvků sítě	2
Lidský faktor	25	Fyzické poškození zařízení	3
	26	Nedodržování směrnic	4
	27	Nedbalost při obsluze zařízení	3
	28	Nedostatečná dokumentace	2
	29	Ztráta důvěrných dat	3
	30	Ztráta přístupového tokenu	3
Neoprávněné činnosti	31	Neoprávněné zkopírování dat	4
	32	Neoprávněný přístup do budovy	2
	33	Vyzrazení Know-How	4
	34	Zneužití uživatelských práv	3
	35	Zneužití administrátorských práv	2

Tabulka 4: Identifikace a hodnocení hrozeb, Zdroj: [Vlastní]

Zranitelnost			IS data	Data	Zálohy	DB data	Reporty	Server	PC	PLC	Výr. Linky	Kamery	NAS	Síťová inf.	OS	Office
Fyzické poškození	1	Požár	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	2	Voda	3	3	3	3	3	4	4	4	4	2	4	3	3	3
	3	Prach	2	2	2	2	2	4	4	4	4	3	4	3	2	2
	4	Chemikálie	2	2	2	2	2	4	4	4	2	1	2	2	1	2
	5	Zničení zařízení	2	2	2	2	2	2	2	4	3	3	4	2	2	2
	6	Exploze	2	2	2	2	2	2	3	5	5	3	2	3	1	2
Dostupnost služeb	7	Výpadek elektrické energie	1	1	1	1	1	1	1	3	3	1	1	1	1	1
	8	Výpadek internetu	1	1	1	2	1	4	2	1	1	2	1	3	1	1
	9	Výpadek IS	3	2	3	3	3	3	3	1	2	3	1	1	1	1
	10	Výpadek serveru	1	4	1	3	1	3	3	1	2	2	4	1	1	1
	11	Výpadek interní sítě	1	2	3	2	3	1	1	2	2	1	2	4	1	1
Důvěrnost služeb	12	Neoprávněný přístup do sítě	4	4	4	4	4	2	1	3	3	2	3	5	1	1
	13	Neoprávněný přístup do IS	4	1	1	4	1	3	4	1	1	2	1	1	1	1
	14	Neoprávněný přístup na server	1	4	1	4	1	2	2	2	2	1	2	1	1	1
	15	Škodlivý software	1	2	4	2	4	2	4	3	1	1	2	3	2	1
	16	Zneužití nebo krádež disků	1	3	3	2	3	3	1	1	1	1	2	1	1	1
	17	Krádež technického vybavení	2	2	2	2	2	3	4	2	2	3	2	1	1	1
	18	Získání dat z vyřazených médií	3	3	3	3	3	2	2	1	1	3	1	1	1	1
Technické selhání	19	Selhání serverů	1	4	2	2	2	2	1	2	2	2	3	1	1	1
	20	Selhání pracovních stanic	1	1	2	1	2	2	3	2	2	1	1	1	1	1
	21	Selhání PLC	1	1	1	1	1	2	1	5	3	4	1	1	1	1
	22	Selhání výrobních linek	1	2	1	1	1	1	1	3	4	1	3	1	1	1
	23	Selhání zálohovacího systému	1	2	4	1	4	1	1	1	1	1	1	1	1	1
	24	Selhání prvků sítě	1	2	3	1	3	1	1	2	1	1	2	1	1	1
Lidský faktor	25	Fyzické poškození zařízení	1	2	3	1	3	2	4	4	4	2	3	4	1	1
	26	Nedodržování směrnic	1	3	3	3	3	1	2	3	3	1	2	3	1	1
	27	Nedbalost při obsluze zařízení	1	2	3	1	3	2	3	4	4	1	2	2	2	1
	28	Nedostatečná dokumentace	3	3	3	4	3	2	2	4	4	2	2	2	1	1
	29	Ztráta důvěrných dat	1	3	3	4	3	1	2	2	3	1	2	1	1	1
	30	Ztráta přístupového tokenu	1	3	3	4	3	2	3	2	2	1	2	2	1	1
Neoprávněné činnosti	31	Neoprávněné zkopírování dat	2	5	5	2	5	2	2	2	2	1	2	1	1	1
	32	Neoprávněný přístup do budovy	1	3	3	1	3	3	3	2	2	1	2	1	2	1
	33	Vyzrazení Know-How	1	3	4	2	4	4	1	3	3	1	1	1	1	1
	34	Zneužití uživatelských práv	2	3	3	3	3	3	3	2	2	1	2	1	2	1
	35	Zneužití administrátorských práv	3	4	4	4	4	4	2	3	3	1	2	3	2	1

Tabulka 5: Matice zranitelností, Zdroj: [Vlastní]

4.1.3 Ohodnocení míry rizika

Hranice rizika jsou rozděleny do pěti skupin:

- Bezvýznamné riziko
- Akceptovatelné riziko
- Mírné riziko
- Nežádoucí riziko
- Nepřijatelné riziko

Hranice pro jednotlivá rizika jsou stanoveny následovně:

Hranice	Riziko
0 – 10	Bezvýznamné riziko
11 – 20	Akceptovatelné riziko
21 – 30	Mírné riziko
31 – 60	Nežádoucí riziko
61 a více	Nepřijatelné riziko

Tabulka 6: Hranice pro hodnocení rizik, Zdroj: [Vlastní]

Teoretická hodnota může být 0 – 125, pro naše potřeby postačí rozmezí 0-100. Hodnoty 100-125 jsou jen teoretické hodnoty, které by nastaly v extrémních případech.

4.1.4 Míra rizika

Teď když máme určena, která rizika chceme chránit, stanovili si hrozby a jejich pravděpodobnost výskytu a následně i jejich zranitelnosti, tak můžeme vypočítat míru rizika. Výsledné hodnoty jsou uvedeny v tabulce a je jim přiřazena patřičná barva podle hranic, které jsme si stanovili v tabulce výše. Použijeme metodu 3 parametrů:

$$Riziko = Pravděpodobnost\ hrozby * Hodnota\ aktiva * Zranitelnost$$

Obrázek 10: Vzoreček pro výpočet míry rizika, Zdroj: [Vlastní]

Riziko			IS data	Data	Zálohy	DB data	Reporty	Server	PC	PLC	Výr. Linky	Kamery	NAS	Síťová inf.	OS	Office
Fyzické poškození	1	Požár	50	50	40	50	40	40	20	40	50	30	40	50	10	20
	2	Voda	15	15	12	15	12	16	8	16	20	6	16	15	3	6
	3	Prach	20	20	16	20	16	32	16	32	40	18	32	30	4	8
	4	Chemikálie	30	30	24	30	24	48	24	48	30	9	24	30	3	12
	5	Zničení zařízení	20	20	16	20	16	16	8	32	30	18	32	20	4	8
	6	Exploze	20	20	16	20	16	16	12	40	50	18	16	30	2	8
Dostupnost služeb	7	Výpadek elektrické energie	15	15	12	15	12	12	6	36	45	9	12	15	3	6
	8	Výpadek internetu	20	20	16	40	16	64	16	16	20	24	16	60	4	8
	9	Výpadek IS	45	30	36	45	36	36	18	12	30	27	12	15	3	6
	10	Výpadek serveru	10	40	8	30	8	24	12	8	20	12	32	10	2	4
	11	Výpadek interní sítě	15	30	36	30	36	12	6	24	30	9	24	60	3	6
Důvěrnost služeb	12	Neoprávněný přístup do sítě	60	60	48	60	48	24	6	36	45	18	36	75	3	6
	13	Neoprávněný přístup do IS	60	15	12	60	12	36	24	12	15	18	12	15	3	6
	14	Neoprávněný přístup na server	15	60	12	60	12	24	12	24	30	9	24	15	3	6
	15	Škodlivý software	20	40	64	40	64	32	32	48	20	12	32	60	8	8
	16	Zneužití nebo krádež disků	10	30	24	20	24	24	4	8	10	6	16	10	2	4
	17	Krádež technického vybavení	30	30	24	30	24	36	24	24	30	27	24	15	3	6
	18	Získání dat z vyřazených médií	30	30	24	30	24	16	8	8	10	18	8	10	2	4
Technické selhání	19	Selhání serverů	15	60	24	30	24	24	6	24	30	18	36	15	3	6
	20	Selhání pracovních stanic	15	15	24	15	24	24	18	24	30	9	12	15	3	6
	21	Selhání PLC	20	20	16	20	16	32	8	80	60	48	16	20	4	8
	22	Selhání výrobních linek	20	40	16	20	16	16	8	48	80	12	48	20	4	8
	23	Selhání zálohovacího systému	10	20	32	10	32	8	4	8	10	6	8	10	2	4
	24	Selhání prvků sítě	10	20	24	10	24	8	4	16	10	6	16	10	2	4
Lidský faktor	25	Fyzické poškození zařízení	15	30	36	15	36	24	24	48	60	18	36	60	3	6
	26	Nedodržování směrnic	20	60	48	60	48	16	16	48	60	12	32	60	4	8
	27	Nedbalost při obsluze zařízení	15	30	36	15	36	24	18	48	60	9	24	30	6	6
	28	Nedostatečná dokumentace	30	30	24	40	24	16	8	32	40	12	16	20	2	4
	29	Ztráta důvěrných dat	15	45	36	60	36	12	12	24	45	9	24	15	3	6
	30	Ztráta přístupového tokenu	15	45	36	60	36	24	18	24	30	9	24	30	3	6
Neoprávněné činnosti	31	Neoprávněné zkopírování dat	40	100	80	40	80	32	16	32	40	12	32	20	4	8
	32	Neoprávněný přístup do budovy	10	30	24	10	24	24	12	16	20	6	16	10	4	4
	33	Vyzrazení Know-How	20	60	64	40	64	64	8	48	60	12	16	20	4	8
	34	Zneužití uživatelských práv	30	45	36	45	36	36	18	24	30	9	24	15	6	6
	35	Zneužití administrátorských práv	30	40	32	40	32	32	8	24	30	6	16	30	4	4

Tabulka 7: Matice rizik, Zdroj: [Vlastní]

4.1.5 Zhodnocení analýzy rizik

O správu dat se stará ICT oddělení, které se řídí směrnicemi, které jim určuje vrcholový management společnosti. Všechny návrhy na změny jsou nejdříve projednávány na úrovni vedení pobočky, po schválení jsou zaslány na projednání managementem společnosti. Toto se týká i nastavení politiky přístupů. Každý ve společnosti může přijít s návrhem či poznatkem na vylepšení. Zálohování dat probíhá na denní bázi na NAS servery, které jsou umístěny v druhé budově, kde sídlí administrativní část. Celý areál je monitorován kamerovým systémem a u vjezdu do areálu se nachází vrátnice. Hlavní nedostatek je v provedení informační infrastruktury v budově, kde se nachází výrobní část. Jsou zde použity prvky, které nevyhovují normám pro průmyslové řešení ISMS. Dále chybí jakékoli oddělení administrativní a výrobní informační části síťové infrastruktury. Toto jsou některé z nedostatků, které musí být odstraněny nebo minimalizovány.

4.2 Návrh síťové infrastruktury

V této kapitole se budeme věnovat již samotnému návrhu sítě. Vše bude navrženo tak, aby byly splněny nároky na průmyslové ISMS.

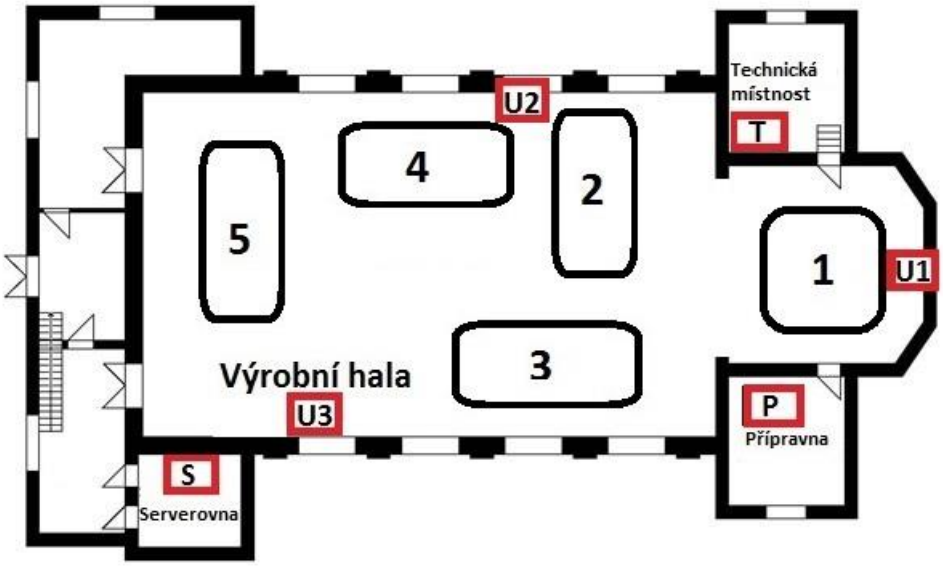
Návrhy zahrnují výběr správných síťových prvků, kabeláže a dalších částí sítě, které jsou svými vlastnostmi vhodné do agresivního průmyslového prostředí. Určíme kabelové trasy, jejich uložení a uzlové body sítě.

Důležité je zajistit co největší dostupnost a kompatibilitu prvků, proto je dobré vybudovat celou síť na komponentech jedné platformy. Pod jednotnou platformu je myšleno, že celá pasivní síť bude od jednoho výrobce. To stejné platí pro aktivní vrstvu. Tento typ řešení nazýváme typizovaným řešením. Aby byla zajištěna nejvyšší možná dostupnost, musíme myslet na redundanci, která pokryje případné výpadky jednotlivých komponent sítě. Abychom byli schopni zajistit vysokou dostupnost a redundanci, bude páteřní síť vybudována do kruhové topologie. Bude se skládat z jednoho hlavního kruhu. Důležité je zastřešit celé řešení pod řídící systém, který umožní rychlý přehled a bude dohlížet na celou síť.

4.2.1 Návrh páteřní sítě a uzlových bodů

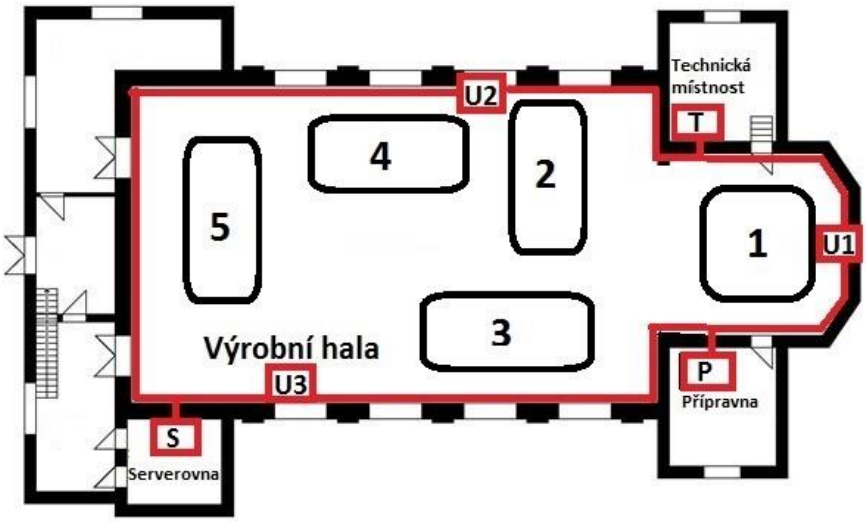
Pod uzlovými body se rozumí aktivní prvky sítě. Ty musí být uzavřeny v datových rozvaděčích, které zajistí, že budou prvky chráněny, před škodlivými vlivy průmyslového prostředí. Pro datové rozvaděče musí být zvoleno takové umístění, které zajistí, že rozvaděče budou dostupné v případě potřeby a nebudou překážet v provozu, aby nedošlo k jejich poškození. Uzlové body je potřeba si pojmenovat. Nejlépe použít označení, která nám už z jejich přečtení usnadní identifikovat, o který bod se jedná, a kde se nachází.

Jak bylo řečeno dříve, páteřní síť bude mít topologii kruhu. Bude mít jeden počáteční uzel, který bude zároveň i uzlem koncovým. Páteřní síť budou tvořit optické kabely, které vyjdou z tzv. Ring mastera, což je hlavní síťový uzel, dále budou procházet přes všechny uzlové body a vrátí se zpět do Ring Mastera. Ring Masterem bude uzlový bod v serverovně.



Obrázek 11: Rozmístění uzlových bodů, Zdroj: [Vlastní]

Když máme rozvrhnuté uzlové body a jejich umístění, musíme je propojit optickým kabelem. Bude se jednat o síť s rychlostí 1Gb/s.



Obrázek 12: Návrh zapojení páteřní sítě, Zdroj: [Vlastní]

Když máme rozmyšlené, jak povedeme páteřní síť, musíme si spočítat, kolik bude potřeba vláken pro zapojení. Pro propojení dvou uzlových bodů, je potřeba dvou vláken:

Výchozí bod	Cílový bod	Počet vláken
S	U3	2 vlákna
U3	P	2+2= 4 vlákna
P	U1	4+2= 6 vláken
U1	T	6+2= 8 vláken
T	U2	8+2= 10 vláken
U2	S	10+2= 12 vláken

Tabulka 8: Výpočet počtu vláken, Zdroj: [Vlastní]

Podle výpočtů bude potřeba 12 vláken pro kompletní zapojení sítě. Nesmíme zapomenout na redundanci, která se určuje na 50% z celkového počtu potřebných vláken. Celkem tedy potřebujeme 18 vláken.

Délka segmentu nepřesáhne 200 metrů a je nutné počítat se svody z vedení trasy a připočítat i rezervu v datových rozvaděčích. Pro tyto účely volíme druh optického kabelu OM2. Kvůli práci s chemikáliemi budou trasy vedeny v kovových lištách, které odolávají vlivu většiny chemikálií, přidělanými podél stěny.

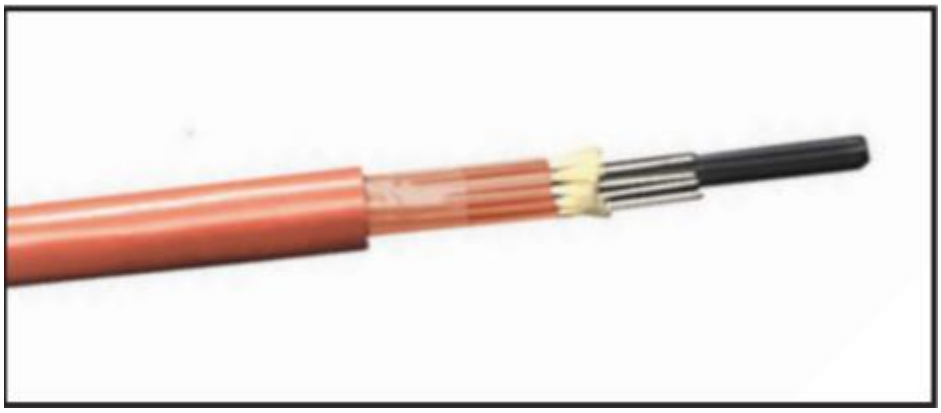
Nyní musíme pro uzlové body zvolit datové rozvaděče. Opět se bude jednat o typizované řešení. Datové rozvaděče musí být přizpůsobené pro použití v průmyslovém prostředí, tedy musí být odolné vůči prachu, vodě a chemickým vlivům. Naše rozvaděče musí splňovat požadavky na 19“ montáž a DIN montáž.

4.2.2 Pasivní vrstva

V této části si ukážeme konkrétní součásti pasivní vrstvy, jako jsou kabely, datové rozvaděče atd.

Optická páteřní síť

Pro optickou síť jsme zvolili kabely od společnosti Belden. Jedná se o optický kabel, který je chráněn polyuretanem, který mu dodává odolnost vůči agresivním vlivům.



Obrázek 13: Optický kabel, Zdroj: [10]

Kabeláž bude vedena v kovových lištách, které ji budou chránit před mechanickým poškozením.

Obrázek 14: Kovová lišta pro vedení kabeláže, Zdroj: [13]

Pro zakončení optických tras použijeme zodolněné konektory, určené pro průmyslové prostředí.

Obrázek 15: Zodolněné konektory pro optické trasy, Zdroj: [3]

Datové rozvaděče

Datový rozvaděč pro průmyslové prostředí je bez ventilátorů či jiných průduchů. Zkušenosti z praxe ukázaly, že uvnitř rozvaděče vzniká stabilní mikroklima, které se výrazně nemění a udržuje stálou pracovní teplotu. Zamezuje také vniku prachu, či jiných částic dovnitř, a následnému zanášení aktivních prvků, které se v něm nacházejí, a je odolný vůči vodě. Námi vybraný je určený pro montáž na zeď.

Obrázek 16: Průmyslový datový rozvaděč, Zdroj:[12]

4.2.3 Výběr aktivních prvků

Výběr správných aktivních prvků pro průmyslovou síť je velice důležitý. Průmyslové aktivní prvky se od těch komerčních liší v tom, že jsou bezventilátorové a zodolněné, aby odolaly agresivnímu průmyslovému prostředí. Chlazení prvků probíhá díky celokovovému obalu, který je dobrý vodič tepla.

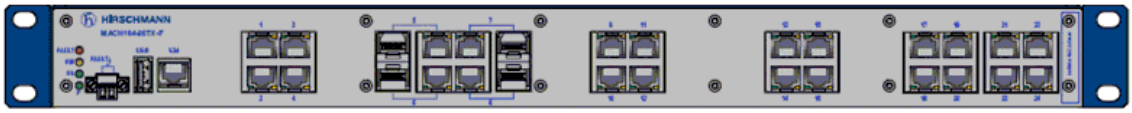
Aktivní prvky pro naše řešení jsme vybrali od společnosti Hirschmann. Osobně jsem tuto společnost navštívil a měl možnost zhodnotit jaká preciznost a pečlivost je vynakládána pro každý výrobek. Obrovský důraz je kladen na kvalitu provedení. Každý jeden kus je ručně i strojně testován, a proto lze s jistotou říct, že jsou to skvělé výrobky, na které se lze spolehnout.

Páteřní switch

Switch musí podporovat rychlost připojení 1Gb/s, a to na všech jeho portech. Vlastnosti switche:

- 19“ palcové provedení
- Podpora topologie Ring
- Plný management
- 24 gigabitových portů
- 4 combo porty

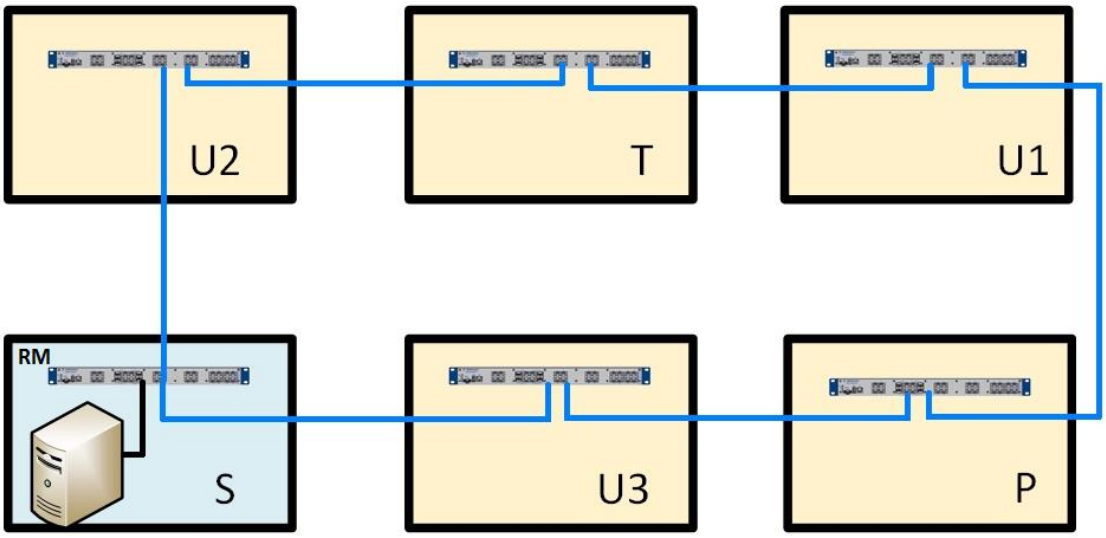
Volba padla na switch MACH 104. Tento switch obsahuje 24 gigabitových portů a k tomu čtyři combo porty. U combo portů se zásuvným modulem lze jednoduše přejít z gigabitového metalického portu na gigabitový optický port. S možností 19“ montáže je vhodnou volbou do našich datových rozvaděčů.



Obrázek 17: Páteřní switch MACH 104, Zdroj:[9]

4.2.4 Blokové schéma zapojení aktivních prvků

V následujícím schématu si zakreslíme zapojení páteřní optické sítě. Jednotlivé uzlové body budou propojeny gigabitovou sítí. Optická páteřní síť je zakreslena modrou barvou. Ring Master je umístěn v serverovně (modrý blok).



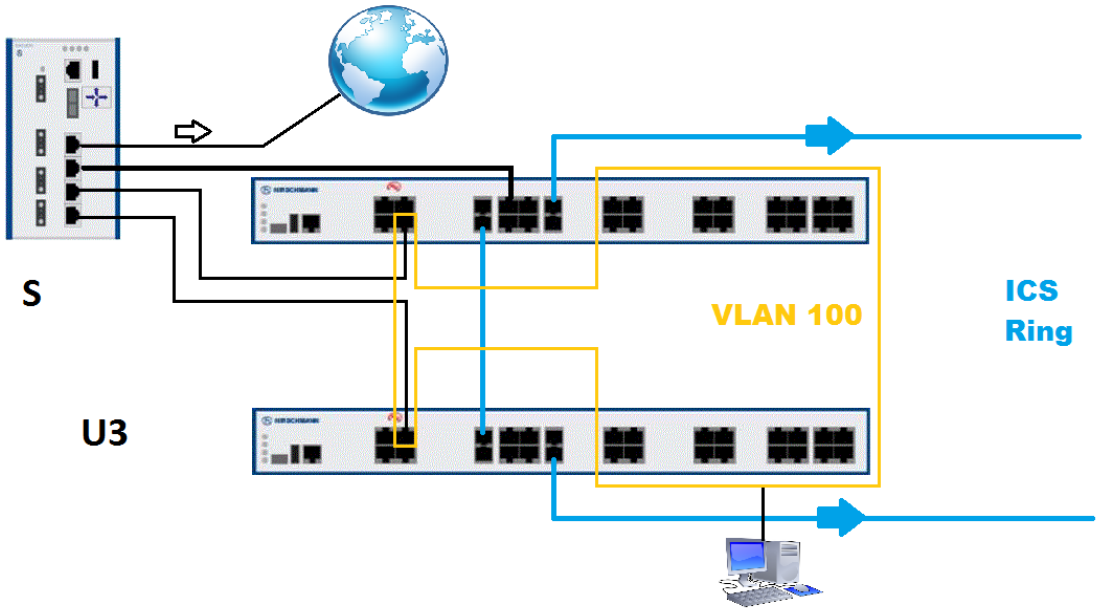
Obrázek 18: Blokové schéma páteřní sítě, Zdroj: [Vlastní]

4.2.5 Oddělení sítí

Nyní si oddělíme administrativní část od výrobní. Do teď byly obě sítě propojené. Toto řešení se nazývá „plochá síť“. Zařadíme tedy routování a nastavíme VLANy, tak abychom obě sítě oddělili. Nastavení VLAN je možné dvojím způsobem: Staticky a Dynamicky. Pro naše řešení zvolíme Statické nastavení.

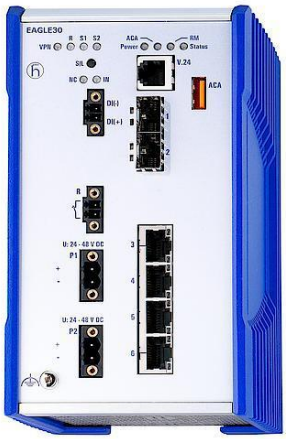
Statické nastavení

Každý port se ručně nastaví v management aktivního prvku. Pokud zapojíme síť do nastaveného portu VLAN, jsme připojeni pouze na konkrétní VLAN a vidíme vše, co se v dané síti nachází. Nevýhodou je, že pokud se stane, že nám někdo přepojí síť na jiný port, ztrácíme spojení s danou sítí. Další nevýhodou může být nedostatečný adresní prostor (rozdělení na L3). Řešením bude zapojení routeru před VLANy.



Obrázek 19: Oddělení adresních prostorů, Zdroj: [Vlastní]

Pro tyto potřeby volíme router Eagle 30 od společnosti Hirschmann. Opět myslíme na typizované řešení. Jedná se o čtyř portový router se základním firewallem. Zvládá gigabitové řešení včetně optických portů. Další funkcionality jsou NAT, VPN, DPI (Deep Packet Inspection). Nesmí chybět WAN port pro komunikaci směrem ven.



Obrázek 20: Router Eagle 30, Zdroj:[14]

4.2.6 Wi-fi řešení

V řešení by se dalo využít pokrytí části výrobní haly pomocí Wi-fi. Nacházíme se ve velice citlivém prostředí. Zpracovávají se zde výbušniny, které jsou citlivé na statickou elektřinu a mikrovlnná záření. Z tohoto důvodu musí být vše perfektně uzemněno. U zaměstnanců je svod elektrostatického náboje řešen pomocí antistatických náramků. Všichni musí nechávat své mobilní telefony bezpečně uzamčené ve skříňkách, to se týká i návštěvníků. Návštěvníci před vstupem do výroby musí podstoupit proceduru, která je zbaví statického náboje. Vstup s mobilním zařízením je přísně zakázán.

Z tohoto důvodu nelze v řešení použít Wi-fi.

4.2.7 Aplikační firewall

Základní řešení firewallu v routeru Eagle 30 je nedostatečné. Pro oddělení kritických procesů použijeme aplikační firewall. Pro tyto potřeby jsme zvolili firewall Tofino Xenon od společnosti Hirschmann. Jedná se o dvouportový firewall s velkou škálou funkcionalit pro zónové řešení. Výhodou je možnost nastavit read-only příkazy do PLC, což se nám bude hodit. Další výhody Tofina:

- Filtrace na L2, L3 a L4 pro všechny Ethernet-based protokolech
- Prevence DoS (Denial of Service) útoků
- Tofino software
- Test mód pro ověřování pravidel firewallu bez ohrožení provozu
- DIN montáž

Tofino využijeme k oddělení kritických výrobních procesů. Před každé PLC výrobní linky zapojíme Tofino, kde nastavíme READ-only příkazy pro PLC, tím pádem zamezíme možnosti náhodného či úmyslného přepsání příkazů u výrobních linek. Dále pomocí Tofina oddělíme kamerový systém.

Obrázek 21: Firewall Tofino Xenon, Zdroj: [15]

4.2.8 Management software

Většina námi zvolených aktivních prvků má buď USB port nebo RJ-11 port, přes který je možné do prvku nahrát konfigurační instrukce. Toto jde udělat i přes síť a k tomu nám poslouží software od firmy Hirschmann. Tímto se vyřeší jednotné řešení aktivních prvků.

HiDiscovery

Produkty Hirschmann jsou dodávány bez defaultní IP adresy, což řeší problém s možnou kolizí adres v síti. Tradiční postup při konfiguraci IP adresy zařízení je připojení sériového portu, ovšem zdaleka ne všechna zařízení tento port mají a to nám pomůže vyřešit HiDiscovery.

HiDiscovery, po instalaci a nakonfigurování, automaticky prohledá LAN a najde všechny Hirschmann zařízení, která jsou k síti připojena, i když nemají ještě nastavenou IP adresu. Pro snadný přehled, se kterým zařízením zrovna pracujeme, poslouží tlačítko „Signal“, které rozsvítí LED indikátor zařízení. Pak už jednoduše odešleme informace po síti rovnou do zařízení.

HiDiscovery dokáže do jisté míry i pomáhat s odhalováním poruch. Například zvýrazněním zařízení, u kterých vzniká kolize IP adres.

Obrázek 22: Ukázka softwaru HiDiscovery, Zdroj: [5]

HiVision

Přehled sítě je předpoklad pro vysokou dostupnost, která je důležitá pro průmyslové ISMS. HiVision slouží ke konfiguraci, správě a dohledu všech Hirschmann zařízení v síti, ale i některých zařízení jiných dodavatelů, které jsou SNMP-enabled.

HiVision je navrženo pro efektivní správu průmyslových sítí a snadno se integruje do SCADA aplikací. Nabízí zabudovaný SNMP-to-OPC server. Jeho grafické uživatelské rozhraní je dostupné jako ActiveX ovládání.

Hlavní funkcionality:

Client/server architektura

- Podpora více klientů zaráz
- Podpora redundantních serverů

Mapa topologie

- Automatické objevení topologie
- Zobrazení stavu zařízení a připojení
- Objeví i zařízení, která lze spravovat

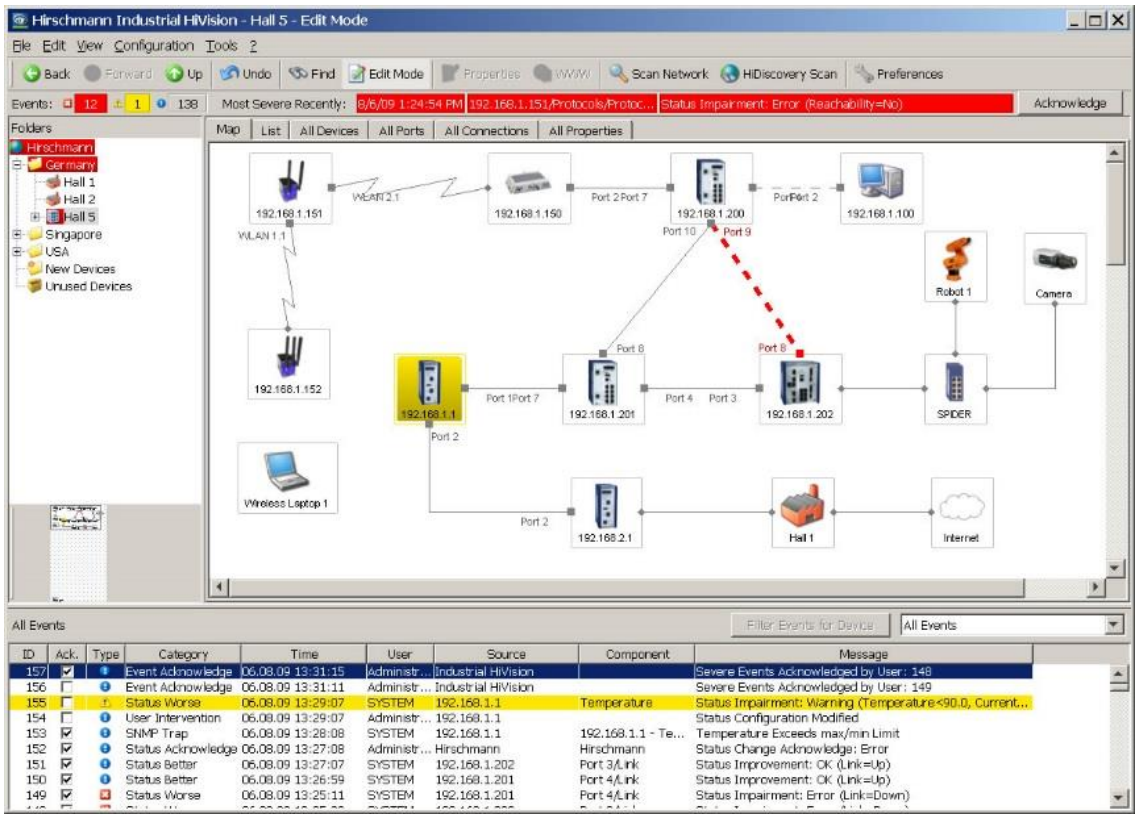
Multiconfig

- Může měnit nastavení i na více zařízení zaráz
- Zařízení nemusí být stejného typu

Event handling

- Nastavitelné logování událostí
- Možný export událostí
- Nastavitelné spouštěče pro události
- Logy dostupné i pro mobilní zařízení (smartphony, tablety atd.)

Integrace do SCADA systémů



Obrázek 23: Ukázka softwaru HiVison, Zdroj: [6]

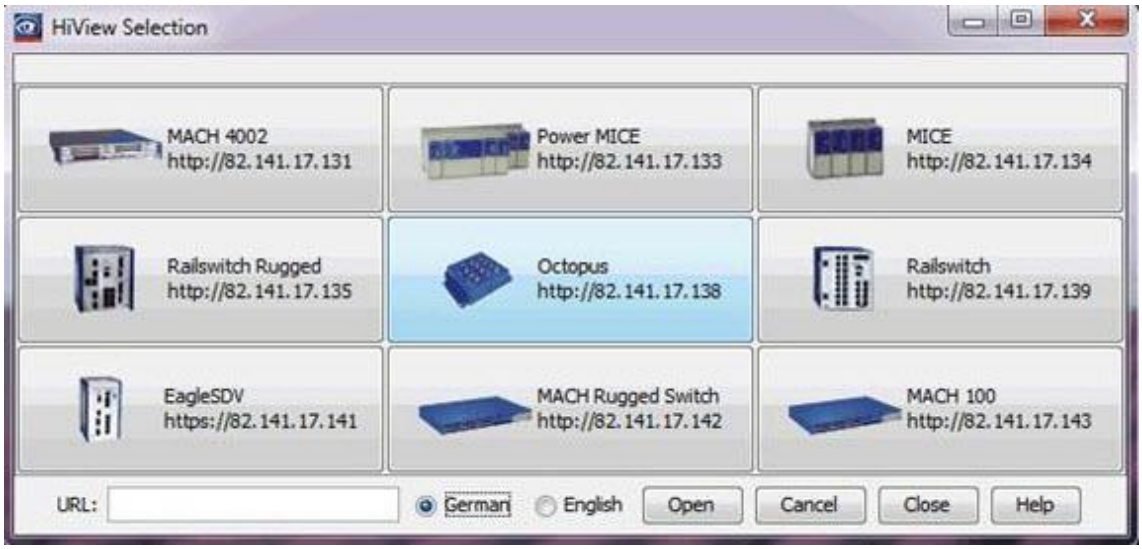
HiView

HiView umožňuje těžit z výhod Hirschmann webových prostředí pro uživatele, bez nutnosti mít nainstalovaný webový prohlížeč nebo JAVU. HiView je portable aplikace, která nevyžaduje instalaci. Může být spuštěna přímo z přenosných USB zařízení jako flash disky nebo SD karty.

Ovládání je velice jednoduché a intuitivní. Seznam naposledy používaných zařízení je zobrazen na obrazovce a ty nejpoužívanější jsou zobrazeny jako první v seznamu. Po kliknutí na požadované zařízení vznikne spojení se zařízením, kdy HiView automaticky vybere nejbezpečnější způsob spojení.

Hlavní funkcionality

- Portable řešení pro opravdu flexibilní užívání
- Seznam naposledy a nejčastěji používaných zařízení
- Přístup k zařízením skrze jejich IP adresu nebo DNS
- Automatický výběr nejbezpečnějšího spojení



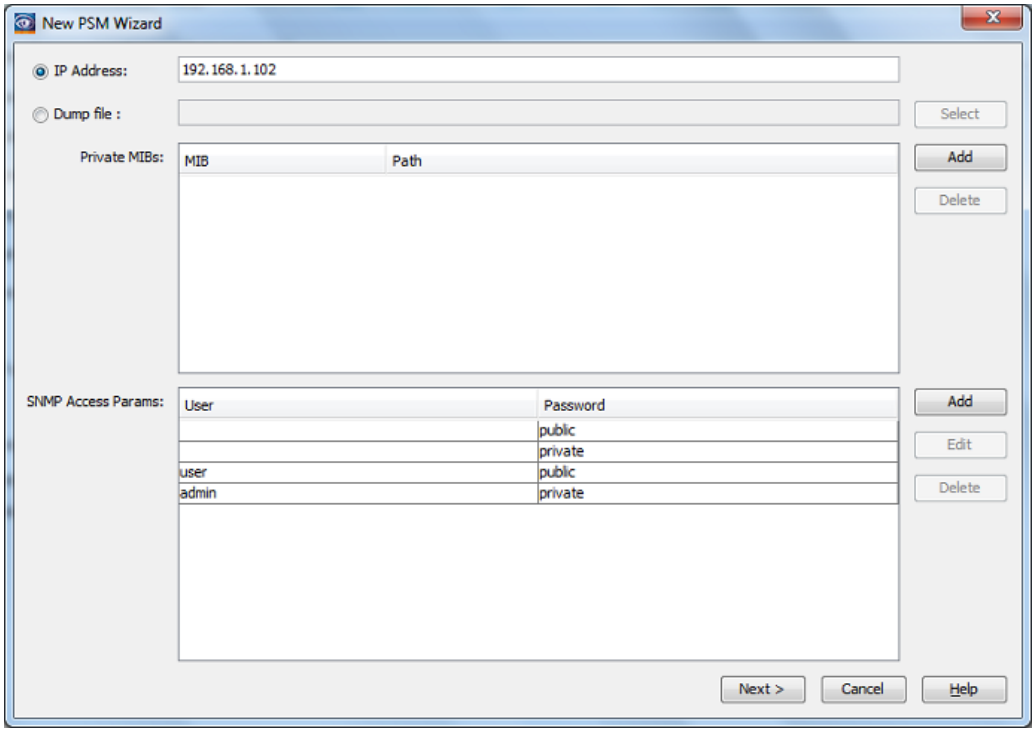
Obrázek 24: Ukázka softwaru HiView, Zdroj: [7]

HiFusion

Dodavatelé aktivních prvků mají širokou škálu MIB proměnných pro svá zařízení, které nepodléhají standartním MIB. HiFusion umožňuje integrovat tato specifická MIB do HiVision softwaru díky vytvoření Product-specific Modules (PSM).

Funguje to tak, že při vytváření PSM pojmenujeme zařízení, definujeme proměnné a přidělíme ikonu zařízení. Další procesy jsou z velké části automatizovány. Nakonec zakomponujeme kompletní PSM do HiVision kdy bude zařízení přidělena ikona a seznam proměnných.

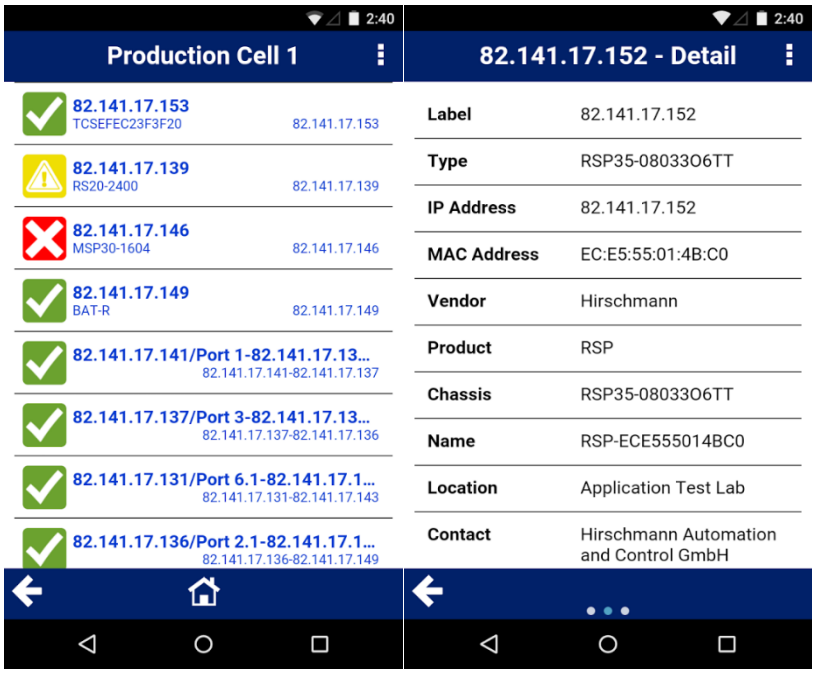
HiFusion je nezávislá aplikace a nevyžaduje tak přítomnost HiVision při vytváření a testování PSM. Jedinou podmínkou je, aby zařízení podporovalo verzi 1 nebo 3 Simple Network Management Protocol (SNMP).



Obrázek 25: Ukázka softwaru HiFusion, Zdroj: [8]

HiMobile

Spojení HiVision a HiMobile je perfektním client/server řešením pro monitoring sítě. Pomocí mobilních zařízení, můžeme udržovat vysokou dostupnost sítě. HiMobile umožňuje přímý přístup ke stavům síťových zařízení prakticky odkudkoli. HiMobile podporuje operační systémy Andriod, Apple iOS a Windows Phone.



Obrázek 26: Ukázka softwaru HiMobile, Zdroj: [9]

4.3 Návrh a zavedení kritických částí ISMS

4.3.1 A.5.1.1. Dokument bezpečnostní politiky informací

ICT tým společně s vedením společnosti sestaví bezpečnostní politiky. Následně v této oblasti vyškolí všechny zaměstnance.

Pověřená osoba: Vedoucí ICT týmu, jednatel společnosti

4.3.2 A.6.1.1. Přidělení odpovědností, A.6.1.2. Koordinace bezpečnosti informací

Je potřeba sestavit směrnici, která bude určovat odpovědnosti v oblasti bezpečnosti informací a zároveň bude koordinovat bezpečnost napříč společností.

V každém týmu bude zvolena jedna zodpovědná osoba, která bude odpovědná za koordinaci při vzniku a řešení bezpečnostních incidentů. Postup při vzniku bezpečnostního incidentu by měl být následovný:

- Vznik incidentu hlásí pracovník svému přímému nadřízenému.
- Ten využije předem stanovených postupů pro jeho řešení.
- Vedoucí pracovník nahlásí incident bezpečnostnímu manažérovi, který incident dále zpracuje.
- Každý incident musí být řádně zdokumentován a musí být zajištěno, že se již nebude opakovat.

Pověřená osoba: Vedoucí ICT týmu, bezpečnostní manažer, vedoucí pracovníci, jednatel společnosti

4.3.3 A.6.1.5. Ochrana důvěrných informací

Informace jsou částečně chráněny pomocí přístupových práv. Je jasně stanovena hierarchie přístupů, která určuje, který pracovník má přístup k jakým datům a jaké operace s nimi může vykonávat. Všichni pracovníci byli seznámeni s těmito pravidly, se sankcemi, které jim budou uloženy, pokud pravidla poruší a podepsali srozumění s těmito pravidly a mlčenlivost o citlivých datech společnosti. Každý pracovník by měl mít přístup jen k takovým datům, které nezbytně potřebuje k výkonu své práce.

Pověřená osoba: Vedoucí pracovníci

4.3.4 A.7.2.2. Povědomí, vzdělávání a školení

Každý pracovník bude vzděláván v informační bezpečnosti, jak zacházet s daty, jak předcházet vzniku bezpečnostních incidentů, jak postupovat při jejich vzniku atd. Zároveň jim bude vysvětlen důvod budování nové infrastruktury, jaký bude mít přínos a vliv na všechny procesy ve společnosti. Dále jim budou objasněny nové funkcionality, které nová infrastruktura nabízí a budou proškoleni ve funkcionalitách, které přímo souvisí s jejich pracovní náplní.

Školení by se měla opakovat v ročním intervalu a každé bude zakončeno formou testu, který musí splnit všichni účastníci. Pokud některý ze zaměstnanců tento test nesplní, bude muset projít školením znovu a test opakovat.

Pověřená osoba: bezpečnostní manažer

4.3.5 A.7.2.3. Disciplinární řízení

Je nutné stanovit formální proces disciplinárního řízení pro případ porušení bezpečnostních směrnic společnosti.

Pověřená osoba: jednatel společnosti, bezpečnostní manažer

4.3.6 A.11.2.4. Údržba zařízení

Je potřeba vytvořit plán pro pravidelnou revizi zařízení. Revize se bude týkat serverů, pracovních stanic, aktivních prvků sítě a záložního zdroje elektrické energie. Pro kontrolu bude vybrán zodpovědný pracovník ICT týmu, který kontrolu provede a zdokumentuje. Nalezené nedostatky nahlásí svému vedoucímu a ten jednateli společnosti. Pro testování záložních zdrojů je potřeba sestavit plán pro měsíční testování.

Pověřená osoba: vedoucí ICT oddělení

4.4 Ekonomické zhodnocení

Protože je ve společnosti potřeba vybudovat novou síťovou infrastrukturu, tzv. od základu, náklady budou vysoké. Komponenty pro průmyslové prostředí jsou dražší než ty pro komerční použití, protože musí vydržet v náročném prostředí průmyslu. Udělejme si souhrn všech potřebných komponent k vybudování sítě.

Položka	Množství	Cena za mj bez DPH	Cena celkem bez DPH
Pasivní vrstva			
Optický kabel OM2	200 m x 12 vláken	45,00 Kč	9 000,00 Kč
Kovová lišta	200 m	98,00 Kč	19 600,00 Kč
Odolné optické konektory	24 ks	499,00 Kč	11 976,00 Kč
Datový rozvaděč	6 ks	9 670,00 Kč	58 020,00 Kč
Aktivní vrstva			
Páteřní switch MACH 104	6 ks	64 890,00 Kč	389 340,00 Kč
Router Eagle 30	1 ks	29 950,00 Kč	29 950,00 Kč
Tofino Xenon	6 ks	58 890,00 Kč	353 340,00 Kč
Management software			
HiVision pro 32 zařízení	1 ks	65 300,00 Kč	65 300,00 Kč
HiView	1 ks	zdarma	-
HiFusion	1 ks	zdarma	-
HiMobile	1 ks	zdarma	-
HiDiscovery	1 ks	zdarma	-
Cena celkem bez DPH a práce			936 526,00 Kč
DPH 21% za materiál			196 671,00 Kč
Práce			350 000,00 Kč
Cena celkem s DPH a prací			1 483 197,00 Kč

Tabulka 9: Rozpočet na realizaci projektu, Zdroj: [Vlastní]

Celkové náklady na komponenty a práci vychází na 1 483 197 Kč. Nejdražší položky jsou prvky aktivní vrstvy. Jedná se ovšem o kvalitní prvky, které odolají i v těch nejtvrdších podmínkách průmyslu. Cenu jednotlivých položek jsme přebrali z praxe po poradě s vedoucím práce.

Těmito komponenty se nám podaří vybudovat novou síťovou infrastrukturu, která bude vyhovovat normám pro průmyslové řešení. Pasivní i aktivní vrstva jsou vybudovány z kvalitních komponent, které zajistí vysokou dostupnost a spolehlivost. Celá síť je zastřešená pod řídícím softwarem, který nám umožní její pohodlné a rychlé nastavení, ale i zabezpečení a pomůže v případě poruchy, kdy jasně označí prvek, který poruchu má. V rámci zachování typizovaného řešení je logické použít software, který pro své prvky dodává přímo společnost Hirschmann. Takže máme zajištěnou 100% kompatibilitu mezi prvky a řídícím softwarem.

4.5 Přínosy navrhovaného řešení

Počáteční investice je vysoká. Zkusme ji porovnat se ztrátami, které by společnosti vznikly, kdyby byla na jeden den ochromena výroba z důvodu ransomwaru.

Po konzultaci s vedoucím práce jsme došli k závěru, že standardní doba na vyřešení bezpečnostního incidentu, který způsobí ransomware, je 1 den. Ransomware je druh malwaru, který zabraňuje přístupu k infikovanému počítači. K opětovnému přístupu je vyžadováno zaplacení výkupného (anglicky ransom).

Od vedení společnosti jsme dostali informace, že denní norma na výrobu rozbušek je 100 000 ks/den. Při ceně 0,7 €/ks to je 70 000 €/den. Při kurzu 26,5 Kč (kurz dle ČNB k 22.5.2017) za 1 € je přepočet roven 1 855 000 Kč/den.

Pokud by takovýto incident nastal, pak by návratnost investice byla 1 den, což je ideální scénář. Ovšem nelze s jistotou říci, že takovýto incident nastane. S investicí do nového řešení infrastruktury se tato pravděpodobnost sníží a z tohoto důvodu, doporučujeme navrhované řešení realizovat.

5 ZÁVĚR

Diplomová práce je rozdělena do tří částí. V první části jsme si stanovili teoretická východiska pro práci. Z těchto východisek jsme čerpali v dalších částech práce.

V praktické části diplomové práce jsme si popsali současný stav ve společnosti. Zjistili jsme, jaké jsou nedostatky. Tyto nedostatky bylo potřeba napravit. Poté jsme si provedli analýzu rizik, kde jsme nejprve udělali seznam všech aktiv společnosti, která musí být zabezpečena. Následně jsme si jednotlivá aktiva ohodnotili. Když už jsme měli seznam aktiv kompletní, mohli jsme se zaměřit na seznam hrozeb a zranitelností pro jednotlivá aktiva. Tyto seznamy jsme pak použili pro sestavení matice rizik, která nám ukázala nejzranitelnější místa aktiv.

Následně jsme již navrhovali samotnou síťovou infrastrukturu. Postupovali jsme od vhodného rozmístění uzlových bodů, přes vedení optických tras až k zapojení celé sítě. Pro realizaci bylo potřeba vybrat vhodné prvky aktivní a pasivní vrstvy. Všechny prvky byly zvoleny tak, aby vyhovovali požadavkům na kvalitu a požadavkům průmyslové bezpečnosti. Dále bylo potřeba oddělit administrativní a výrobní časti sítě a zónové zabezpečení kritických procesů pomocí aplikačního firewallu. Následně jsme celé řešení zastřešili pod management software, který bude sloužit k jednoduchému a rychlému nastavení sítě, k monitoringu a hlášení výpadků či nedostatků v síti.

V poslední části jsme si zavedli nejkritičtější části ISMS, které jsme vyhodnotili z analýzy rizik.

To vše jsme zhodnotili v ekonomické rozvaze, kde jsou zaznamenány jednotlivé položky včetně jejich ceny. Celkové náklady na řešení jsme porovnali s denními ztrátami v případě bezpečnostního incidentu, který by na celý den vyřadil provoz.

Navržené řešení v diplomové práci bude sloužit jako zadání pro výběr dodavatele.

6 SEZNAM POUŽITÉ LITERATURY

[1] ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. 1. vyd. Brno: CERM, Akademické nakladatelství, 2013. ISBN 978- 80-7204-872-4.

[2] JORDÁN, V. a V. ONDRÁK. *Infrastruktura komunikačních systémů II: Kritické aplikace*. 1. vyd. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5240-4.

[3] SEDLÁK, P. *Technologická bezpečnost ICT.* Přednáška. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská: akademický rok 2015/2016.

[4] JORDÁN, V. a V. ONDRÁK. *Infrastruktura komunikačních systémů III: Integrovaná podniková infrastruktura*. Brno: CERM, Akademické nakladatelství, 2016. ISBN 978-80-214-5241-1.

[5] BELDEN. *Belden.com* [online]. [cit. 23.4.2017]. Dostupný na WWW: http://www.belden.com/blog/industrialethernet/images/HiDiscoveryScreenShotImage.jpg

[6] HIRSCHMANN. *Hivision.de* [online]. [cit. 23.4.2017]. Dostupný na WWW: http://www.hivision.de/res/Media/hivision.de/Medien/Images/Industrial_HiVision_4.0Industrial_HiVision_v40.jpg214162.jpg

[7] DAANET. *daanet.com* [online]. [cit. 23.4.2017]. Dostupný na WWW: http://daanet.com.au/media/56/1437649325.HiViewScreenshot.jpg

[8] GAE. *gae.co.id* [online]. [cit. 23.4.2017]. Dostupný na WWW: http://www.gae.co.id/userdata/uploads/product/bab0e4c7f604c74f9864d196cc3cabdf.png

[9] MOBOMARKET. *mobomarket.net.* [online]. Copyright © 2016 [cit. 23.4.2017]. Dostupné z: http://m.mobomarket.net/free-download-himobile-4294179361.html

[10] FIBER CATALOG. *Belden.com* [online]. [cit. 23.4.2017]. Dostupný na WWW: http://info.belden.com/hs-fs/hub/282305/file-403328970-pdf/Belden-Optical-Fiber-Catalog-12.13.pdf

[11] QCOM. *qcom.cz* [online]. © 2016 [cit. 19.5.2017]. Dostupné z: http://www.qcom.cz/home/cesky/systemy_rizeni/isms/struktura_27k.gif

[12] TRITON. *triton.cz* [online]. [cit. 23.4.2017]. Dostupné z: http://www.triton.cz/userfiles/image/SAD/2015/SAD_1.jpg

[13] MADER. *mader.cz* [online]. [cit. 23.4.2017]. Dostupné z: https://www.mader.cz/cable-manager-1u-60x40-2m-black

[14] MI GROUP. *mi-group.eu* [online]. [cit. 25.4.2017]. Dostupné z: http://www.migroup.eu/fileadmin/_processed_/csm_p_ik_EAGLE_30_5702cfa58a.jpg

[15] INS. *industrialnetworking.com* [online]. © 2016 [cit. 25.4.2017]. Dostupné z: http://www.industrialnetworking

7 SEZNAM TABULEK

8 SEZNAM OBRÁZKŮ

9 Seznam zkratek a pojmů

Aktivní vrstva - všechna zařízení, která slouží ke vzájemnému propojení v počítačových sítích. Aktivní síťový prvek je všechno to, co nějakým způsobem aktivně působí na přenášené signály – tedy je zesiluje a různě modifikuje. Mezi aktivní prvky se řadí především opakovač, hub, switch, bridge nebo router. Patří zde však i další zařízení jako například síťová karta, tiskový server nebo host adapter.

DIN lišta - v elektrotechnice označení pro kovovou lištu normalizovaného tvaru a rozměrů. Lišty slouží k upevňování elektrických přístrojů v rozvodnicích, rozvaděčích, ovládacích skříních a podobných zařízeních. Na nosnou lištu mohou být přístroje nasunuty zboku nebo nacvaknuty zepředu a zaaretovány.

DNS – Domain Name Systém je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. Později ale přibral další funkce (např. pro elektronickou poštu či IP telefony) a slouží dnes de facto jako distribuovaná databáze síťových informací.

DoS – Denial of Service, český překlad „odepření služby“. Je to typ útoku na internetové služby nebo stránky, jehož cílem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům. Může k tomu dojít přehlcením požadavky či využitím nějaké chyby, která sice útočníkovi neumožní službu ovládnout, ale umožní ji rozbít.

DPI – Deep Packet Inspection, volně přeloženo jako „hloubková kontrola paketu“. Jedná se o formu filtrování paketů v počítačové síti, která zkoumá datovou část (a případně i záhlaví) paketu při procházení inspekčním bodem. Hledá nesoulad s protokolem, viry, spam, vniknutí nebo definovaná kritéria, aby rozhodl, zda paket může projít, nebo je-li třeba jej směřovat do jiného určeného místa. Může sloužit i pro účely shromažďování statistických informací, které fungují na aplikační vrstvě OSI modelu.

Ethernet - je název souhrnu technologií pro počítačové sítě pro komunikaci přenosovými rychlostmi od 1 Mbit/s po 100 Gbit/s. Sítě Ethernet realizují fyzickou a linkovou vrstvu referenčního modelu OSI, takže je možné po nich provozovat jeden nebo více protokolů

síťové vrstvy, především protokoly IPv4 a IPv6, které se používají pro služby sítě Internet.

HW - Hardware označuje fyzické vybavení počítače.

L2, L3 a L4 – označení pro druhou (linkovou), třetí (síťovou) a čtvrtou (transportní) vrstvu referenčního modelu ISO/OSI. Referenční model ISO/OSI se používá jako názorný příklad řešení komunikace v počítačových a telekomunikačních sítích pomocí vrstevnatého modelu, kde jsou jednotlivé vrstvy nezávislé a snadno nahraditelné.

MIB - Management Information Base popisuje sadu objektů, které jsou předmětem správy. Spravované zařízení může implementovat jednu nebo více MIB, v závislosti na jeho funkci. Tyto MIB databáze jsou velmi podobné standardním databázím v tom smyslu, že popisují jak strukturu, tak formát dat.

NAS – Network Attached Storage – volně přeloženo jako „datové úložiště na síti“. V informatice označení pro datové úložiště připojené k místní síti LAN. Data tohoto úložiště mohou být poskytována různým uživatelům. NAS nemusí mít pouze funkci souborového serveru, ale může mít i jiné specializované funkce.

NAT – Network Adress Translation, český překlad je „překlad síťových adres“. V počítačových sítích se jedná o způsob úpravy síťového provozu procházejícího přes router přepisem zdrojové nebo cílové IP adresy, případně i hlaviček protokolů vyšší vrstvy

Pasivní vrstva – Horizontální a páteřní kabeláž sítě.

PLC – Programmable Logic Controller, český překlad „ programovatelný logický automat“. Jedná se o relativně malý průmyslový počítač, používaný pro automatizaci procesů v reálném čase – řízení strojů nebo výrobních linek v továrně.

Revize - se zabývají kontrolou, správou a evidencí veškerých zařízení.

SCADA - Supervisory Control And Data Acquisition, český překlad „dispečerské řízení a sběr dat“. Obvykle se tento pojem používá pro software, který z centrálního pracoviště monitoruje průmyslová a jiná technická zařízení a procesy a umožňuje jejich ovládání.

SNMP - Simple Network Management Protocol je součástí sady internetových protokolů. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě, a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě.

SW – Software sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost.

Topologie - Topologie sítí se zabývá zapojením různých prvků do počítačových sítí a zachycením jejich skutečné (reálné) a logické (virtuální) podoby (datové linky, síťové uzly)

UTP – Unshielded Twisted Pair, český překlad „nestíněný kroucený pár“. Kroucený pár je druh kabelu, který je používán v telekomunikacích a počítačových sítích. Kroucená dvojlinka je tvořena páry vodičů, které jsou po své délce pravidelným způsobem zkrouceny a následně jsou do sebe zakrouceny i samy výsledné páry

VLAN – Virtual Local Area Network, přeloženo jako „Lokální virtuální síť“. Jedná se o logicky nezávislou síť v rámci jednoho nebo několika zařízení.

VPN – Virtual Private Network, český překlad „virtuální privátní síť“. V informatice prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné.

WAN – Wide Area Network, český překlad „rozsáhlá síť“. V informatice se takto označuje počítačová síť, která pokrývá rozlehlé geografické území (například síť, která překračuje hranice města, regionu nebo státu). Největším a nejznámějším příkladem sítě WAN je síť Internet.